

RESEARCH REPORT

**#010**

The background of the cover features a complex network diagram. It consists of numerous small blue dots (nodes) connected by thin, light blue lines (edges). The nodes are scattered across the frame, with a higher density in the lower right quadrant. The overall effect is a sense of interconnectedness and complexity, typical of a network graph or data visualization. The background is a dark blue gradient.

# Negative Multiplicity: Forecasting the Future Impact of Emerging Technologies on International Stability and Human Security



# Table of Contents

|  |           |
|--|-----------|
| List of Abbreviations                          | 4         |
| Abstract                                       | 5         |
| Funding  | 5         |
| Acknowledgements                               | 6         |
| Executive Summary                              | 7         |
| Main Results                                   | 8         |
| <b>1 Introduction</b>                          | <b>11</b> |
| <b>2 Methods</b>                               | <b>16</b> |
| 2.1 Definitions                                | 16        |
| 2.2 Data Collection                            | 20        |
| 2.3 Data Analysis and Visualisation            | 29        |
| 2.4 Limitations                                | 30        |
| <b>3 Findings</b>                              | <b>33</b> |
| 3.1 Technology Forecasting                     | 33        |
| 3.2 Technology Impact Assessment               | 37        |
| 3.2.1 Technologies' Individual Impact          | 37        |
| 3.2.2 Technology Clusters                      | 44        |
| 3.2.3 Acuteness                                | 46        |
| <b>4 Conclusions</b>                           | <b>49</b> |
| Endnotes                                       | 54        |
| References                                     | 57        |
| Data Annex                                     | 63        |
| 1 AI for C4ISR                                 | 63        |
| 2 AI for Weapons and Effects                   | 67        |
| 3 AI for Cyber Operations                      | 71        |
| 4 AI for Information Warfare                   | 75        |
| 5 Quantum for Hardening and Exploiting Systems | 79        |
| 6 Quantum for C4ISR                            | 83        |
| 7 ASAT Capabilities                            | 87        |
| 8 Hypersonic Weapon Systems                    | 91        |
| 9 Directed Energy Weapons                      | 95        |
| 10 Physical Human Enhancement Technologies     | 98        |
| 11 Cognitive Human Enhancement Technologies    | 101       |
| 12 Synthetic Biology                           | 105       |

## List of Abbreviations

|                  |   |
|------------------|---|
| <b>2D</b>        | Two-Dimensional   |
| <b>3D</b>        | Three-Dimensional   |
| <b>4IR</b>       | Fourth Industrial Revolution  |
| <b>A2/AD</b>     | Anti-Access/Area-Denial   |
| <b>AI</b>        | Artificial Intelligence   |
| <b>ASAT</b>      | Anti-Satellite  |
| <b>BMD</b>       | Ballistic Missile Defence   |
| <b>BWC</b>       | Biological Weapons Convention   |
| <b>C4ISR</b>     | Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance |
| <b>COVID-19</b>  | Coronavirus Disease 2019  |
| <b>CRISPR</b>    | Clustered Regularly Interspaced Short Palindromic Repeats                                   |
| <b>DEWs</b>      | Directed Energy Weapons   |
| <b>GPS</b>       | Global Positioning System   |
| <b>HET</b>       | Human Enhancement Technologies  |
| <b>ISR</b>       | Intelligence, Surveillance, and Reconnaissance  |
| <b>IoT</b>       | Internet of Things  |
| <b>IT</b>        | Information Technology  |
| <b>ML</b>        | Machine Learning  |
| <b>NATO</b>      | North Atlantic Treaty Organization  |
| <b>NC3</b>       | Nuclear Command, Control, and Communications  |
| <b>New START</b> | New Strategic Arms Reductions Treaty  |
| <b>NPT</b>       | Treaty on the Non-Proliferation of Nuclear Weapons  |
| <b>R&amp;D</b>   | Research and Development  |
| <b>STREAM</b>    | Systematic Technology Reconnaissance, Evaluation, and Adoption Methodology                  |
| <b>TPNW</b>      | Treaty on the Prohibition of Nuclear Weapons  |
| <b>TRL</b>       | Technology Readiness Level  |
| <b>UN</b>        | United Nations  |

## Abstract

We asked 30 experts to forecast the developmental trajectories of twelve emerging technologies in the United States, Russia, and China until 2040 and to score their possible future impact on arms race stability, crisis stability, and humanitarian principles. The results reveal that, on average, their impact is expected to be negative, with some technologies negatively affecting all three dependent variables. We used a machine learning algorithm to cluster the technologies according to their anticipated impact. This process identified technology clusters comprised of diverse high-impact technologies that share key impact characteristics but do not necessarily share technical characteristics. We refer to these combined effects as ‘negative multiplicity’, reflecting the predominantly negative, concurrent, and in some cases similar, first- and second-order effects that emerging technologies are expected to have on international stability and human security. The expected alignment of the technology development trajectories of the United States, Russia, and China by 2040, in combination with the negative environment created by geopolitical competition, points to a nascent technological arms race that threatens to seriously impede international arms control efforts to regulate emerging technologies.

**Keywords:** Emerging technologies, international stability, human security, forecasting, arms control

## Funding

This study received funding from the German Federal Foreign Office through the 2019–2022 project grant ‘Arms Control and Emerging Technologies’ (‘Forschungs- und Transferprojekt Rüstungskontrolle und Neue Technologien’).

## Acknowledgements

We would like to extend our sincere thanks to a few individuals who made significant contributions to this study. Our research assistant, Beatrice von Braunschweig, led the literature review and provided valuable support at several key points throughout the project. Richard Flint contributed to the data analysis, generated data visualisations, and created the website for this report. Our colleagues Michael Brzoska, Marten Ennen, Alexander Kelle, Moritz Kütt, Holger Niemann, Jantje Silomon, and Tim Thies contributed to this study at various stages. James Black, Ingvild Bode, Ben Loehrke, Frank Sauer, and Maaïke Verbruggen provided feedback on the technology scoring criteria. Jessica Bland, Mischa Hansel, and Heather Williams gave insightful comments on a draft of this report. Finally, we thank all the experts who participated in the technology scoring exercise and qualitative debriefs.

## Executive Summary

The military applications of a new generation of technologies have given rise to significant concerns regarding their potential impact on international stability and human security. Meanwhile, decision makers who aim to mitigate these concerns through arms control measures face an uphill battle: the speed of technological innovation, the unclear impact of emerging technologies, and intensifying military-technological competition between the United States and Russia and China are impeding effective arms control for emerging military technologies.

This report is the capstone of a one-year study with the objective of forecasting the impact of emerging technologies on international stability and human security. It answers three questions:

1. What impacts are emerging technologies likely to have on arms race stability, crisis stability, and humanitarian principles up to 2040?
2. Which emerging technologies show similarities in terms of impact?
3. When will the impact of these technologies become most acute?

We asked 30 international experts to evaluate the military applications of twelve emerging technologies. First, we had them to assess the current and expected maturity of each technology over the next twenty years. We then asked them to answer 54 questions about each technology's expected positive and negative impact and gave them an opportunity to provide qualitative comments. We limited the questions on arms race and crisis stability to the U.S.–Russian and U.S.–Chinese nuclear dyads insofar as we expect these countries to have an outsized influence on peace and security over the next twenty years. We then applied a machine learning algorithm to cluster all the quantitative data points from the survey (~8,000) to identify similarities and differences between the technologies' effects. This process helped us to identify five technology clusters, which we visualised in three-dimensional graphs on an accompanying webpage: [www.negative-multiplicity.com](http://www.negative-multiplicity.com). The study concluded with the collection of a second round of qualitative data from experts' debriefs.

## Main Results

According to the experts surveyed:

- All twelve technologies will reach operational deployability by 2040 in the United States, Russia, and China. By then, these technologies are expected to be useable on the battlefield.
- Hypersonic weapon systems and directed energy weapons will make a significant jump in terms of their deployability by 2030. For hypersonic weapon systems, this could be reflective of an ongoing arms race.
- All twelve technologies will weaken either international stability or human security, and half of the technologies examined will predominantly weaken (rather than strengthen) both. The net impact of all the technologies was negative.
- Anti-satellite capabilities and AI-enhanced information warfare show uniquely negative impacts, particularly for crisis stability. Their possible second-order effects on human security raise serious concerns.
- AI and quantum technologies for command, control, communications, computers, intelligence, surveillance, and reconnaissance purposes are expected to have the most positive effects of any of the examined technologies. By increasing clarity and situational awareness, these military applications could strengthen crisis stability.
- Similarities in impact do not necessarily mirror technological similarities. Some technologies have very similar effects on international stability and human security, though they share no technical characteristics with one another.
- Great power competition will be the main driver behind future research and development in the United States, Russia, and China. A possible China-Russia alliance could confront the United States with serious military-technological challenges.

We term these combined effects ‘negative multiplicity’, reflecting the predominantly negative, concurrent, and in some cases, similar first- and second-order effects that emerging technologies are expected to have on international stability and human security (see Table I).



**Table I: Strengthening/weakening effects for every technology, on each axis**

| TECHNOLOGY                                   | ARMS RACE STABILITY | CRISIS STABILITY | HUMANITARIAN PRINCIPLES | OVERALL RESULT |
|--|---------------------|------------------|-------------------------|----------------|
| AI for C4ISR                                 | Strengthen          | Strengthen       | Weaken                  | Mixed          |
| AI for weapons and effects                   | Weaken              | Weaken           | Weaken                  | Weaken         |
| AI for cyber operations                      | Weaken              | Weaken           | Weaken                  | Weaken         |
| AI for information warfare                   | Weaken              | Weaken           | Weaken                  | Weaken         |
| Quantum for hardening and exploiting systems | Weaken              | Strengthen       | Weaken                  | Mixed          |
| Quantum for C4ISR                            | Weaken              | Strengthen       | Strengthen              | Mixed          |
| ASAT capabilities                            | Weaken              | Weaken           | Weaken                  | Weaken         |
| Hypersonic weapon systems                    | Weaken              | Weaken           | Weaken                  | Weaken         |
| DEWs   | Weaken              | Weaken           | Weaken                  | Weaken         |
| Physical HET                                 | Weaken              | Strengthen       | Weaken                  | Mixed          |
| Cognitive HET                                | Weaken              | Strengthen       | Weaken                  | Mixed          |
| Synthetic biology                            | Weaken              | Strengthen       | Weaken                  | Mixed          |

Our clustering exercise revealed that the technology cluster with the most negative impact on international stability and human security consists of technologies that share few – if any – technical characteristics. We thereby conclude that a narrow research or policy focus on a single technology or a single area of impact obscures the similar effects of seemingly dissimilar technologies. Such a narrow focus also risks obscuring the significant second-order effects on human security that their use could generate. These issues become more pronounced when one considers those technologies that are expected to mature more rapidly over the next ten years. For example, the expected jump in the deployability of hypersonic weapon systems and directed energy weapons is worrying. For hypersonic weapon systems, this rapid change in deployability could reflect and exacerbate perceptions of an already ongoing arms race.

Our study underscores the negative environment created by geopolitical competition. Combined with the expected extent of technology trajectory alignment between the United States, Russia, and China, we find evidence of an ongoing arms race for emerging military technologies. Consequently, future arms control efforts will likely face resistance from the great powers, and existing agreements might come under additional pressure. Inversely, the expected technological alignment of the three countries could benefit arms control efforts. Arms control may seem more attractive when adversaries begin to close the competitive gap. In any case, technology governance in light of negative multiplicity will require recognising the interactive potential of emerging technologies. The window for preventive initiatives could soon close, however, if the deployability forecasts of our experts are correct.

# 1 Introduction

The pace and scope of technological innovation has led some to conclude that humanity is experiencing a ‘fourth industrial revolution’ (4IR). According to a United Nations (UN) report, ‘[d]riving the 4IR forward are rapid advances in digital technologies – artificial intelligence (AI), machine learning, robotics, additive manufacturing (3D printing), the Internet of Things (IoT), distributed-ledger technology [...] or blockchain, and quantum computers – and their integration with biotechnology, nanotechnology and cognitive, social and humanitarian sciences’ (UNIDO 2019: 1).

The emergence of this new generation of technologies has already impacted international peace and security. In the war in Ukraine, remotely operated aerial platforms have played a crucial role for both sides’ militaries, and Russian forces claim to have used new high-precision hypersonic missiles (Reuters 2022). As with earlier industrial revolutions, the military applicability of emerging technologies will lead to new weapons, new military capabilities, new strategies and military doctrines, and new or changed political expectations (Schneider and Macdonald 2022). Still, the impacts of emerging technologies do not materialise in a vacuum. Whether the impact of these innovations on international peace and security will be mostly negative or positive also depends on the social and political contexts in which these technologies are embedded (cf. Kranzberg 1986: 547). Economic factors and international competition can have both positive and negative effects on innovation and regulation (Cozzens et al. 2010: 361; Kavanagh 2019: 37; van Hooft, Boswinkel, and Sweijs 2022: 7). Attitudes among politicians and military leaders are also likely to significantly influence a given technology’s impact (Onderco and Zutt 2021).

The conventional wisdom, in both policy and military circles, is that the impact of emerging technologies will be significant. U.S. President Joe Biden anticipates that we will see ‘more technological change in the next 10 years than we saw in the last 50. That’s how rapidly artificial intelligence and so much more is changing’ (The White House 2021). The U.S. Secretary of Defence has stressed that ‘[e]merging technologies must be central to our strategic development’ (U.S. Department of Defense 2021). Referring to AI, Russian President Vladimir Putin famously predicted that ‘[w]hoever becomes the leader in this sphere will become the ruler of the world’ (quoted in Vincent 2017). He simultaneously cautioned that AI ‘comes with colossal opportunities, but also threats that are

difficult to predict' (ibid.). Whilst China's State Council pledged that China would become the 'premier global AI innovation centre' by 2030 (quoted in Kania 2017), the Chinese envoy to the UN also warned that '[t]he rapid development of the military application of AI may give rise to security, humanitarian, legal and ethical concerns' (Permanent Mission 2020). The UN Secretary-General argues that emerging technologies could blur the lines between war and peace (United Nations 2021), and the UN High Representative for Disarmament Affairs has warned that emerging technologies 'are evolving faster than our normative, legal and regulatory structures' (UNODA 2019).

These concerns have been echoed by international security studies and think tank experts concerned with global security affairs. Scholars have long sought to make sense of rapid technological change and its impact on peace and security. Today, many scholarly accounts concentrate on the impact of a single technology, such as AI (cf. Ayoub and Payne 2016; Boulanin 2019; Saalman 2019) or limit their focus to a single impact, such as strategic stability (cf. Chyba 2020; Cox and Williams 2021; Johnson 2019, 2021; Kroenig 2021). Studies on the humanitarian effects of emerging technologies often omit strategic stability considerations, and vice versa (cf. Beard 2018; Rejali and Heiniger 2020; Shebab 2022; Swanson 2010). What this division obscures, however, is the degree to which international stability and human security can inform and shape one another in the context of emerging technologies. Strategic instability, for instance, is almost always a challenge to human wellbeing, particularly if such instability becomes a catalyst for (nuclear) war. Likewise, an improved ability to comply with humanitarian principles through the use of new technologies could paradoxically decrease crisis stability by lowering the threshold of resorting to conventional weapons use in the first place (Ministry of Defence 2015: 31–32). The relationship between international stability and human security is far from obvious and would benefit from further research evaluating the linkages and interactions between these two spheres of peace and security.

Meanwhile, more comprehensive accounts of different technologies regularly consider their potentially positive effects from a state- or alliance-centric military perspective while leaving aside their potentially negative effects, for instance on arms control (cf. NATO 2020; Scharre and Riikonen 2020). Despite the variety of technologies in the military sector, 'trending topics' such as AI and drones (Ayoub and Payne 2016; Brundage et al. 2018; Byman 2013; Johnson 2021; Müller and Bostrom 2016) and hypersonic missiles (Acton 2014; Kunertova

2021; Williams 2019) receive comparably more attention than biotechnology or quantum technologies (Horowitz 2020: 387).

Excessively siloed debates and analyses risk failing to account for the potentially *multiple* and *intertwined* effects of emerging technologies at both the international and the human level. These effects could include, but are not limited to, the entanglement of legacy military systems with emerging technologies to the detriment of crisis stability (Acton 2018), the cumulative effects of several co-existing technologies (Sechser, Narang, and Talmadge 2019), or the effects created by the interaction of new technologies on the battlefield (European Parliament Research Service 2021).

Political decision makers are facing a highly dynamic and complex technological environment, one that is difficult to comprehend and react to. The dual-use capacity of many emerging technologies (i.e., their parallel applicability for civilian and military purposes) and the occasionally opposing interests of global corporations and private consumers complicate political choices. This is particularly evident to those decision makers concerned with mitigating the negative effects of emerging technologies through multilateral arms control initiatives. In such cases, those in positions of influence may struggle to focus their limited resources on effective policies (cf. UNODA 2019).

These developments are also taking place in an international environment marred by high geopolitical tension. ‘Great power competition’ – the (renewed) rivalry between the United States and its allies on the one hand and Russia and China on the other – has complicated efforts by the international community to meaningfully regulate some of the most concerning technologies. For example, many states are interested in regulating the use and proliferation of lethal autonomous weapons systems. Negotiations at the UN level remain stuck, however, due in part to the continued interest of great powers in these weapons platforms, which is underpinned by perceptions of asymmetric advantage (Sauer 2021). Finally, in recent years, a negative perception of arms control has taken hold in both Moscow and Washington (Wisotzki and Kühn 2021).<sup>1</sup>

This context motivated us to provide a systematic assessment of the future impact of emerging technologies. We applied a novel three-dimensional perspective to gauge the future impact of emerging technologies on arms race stability, crisis stability, and humanitarian principles. Our starting premise was twofold: first,

there is a new generation of emerging technologies with (potential) military applicability; second, these technologies could individually, and in some cases, collectively impact international stability and human security to a degree that is worth evaluating.

We believe that the aforementioned siloing of particular technologies and their impact in academic and policy debates undermines efforts to properly navigate the broader technological landscape. Novel technologies are not emerging sequentially; they are developing together and interacting with each other, as are the challenges and opportunities that they represent for international stability and human security. The likelihood of an intensified arms race, crisis instability, and the violation of humanitarian principles in the coming years cannot be evaluated based on a single innovation. What is needed is a sense of the potential impact of multiple technologies that are currently being developed in unison, albeit at different paces.

In this report, we evaluate: 1) the possible future impact of twelve specific emerging technologies on arms race stability, crisis stability, and humanitarian principles by the year 2040; 2) which emerging technologies show similarities in terms of impact; and 3) when the impact of these technologies might become most pronounced. We relied on expert opinion to forecast the future impact of twelve military applications of emerging technologies. The impact questions – particularly questions relating to international stability – were focused on the United States, Russia, and China. We then applied a machine learning (ML) algorithm to cluster all the quantitative data points (~8,000) to identify similarities and differences between the technologies' anticipated impacts. We added to this a round of qualitative data collection to gain a deeper understanding of the experts' predictions. The survey was conducted prior to Russia's invasion of Ukraine on 24 February 2022.

The target audience of the study is scholars and decision makers. Our ambition is to bridge the gap between different academic siloes in research on emerging technologies and to provide a multi-perspective approach to analysing the impact of such technologies. By clustering technologies by effect, we hope to improve on some of the more traditional ways of thinking about emerging technologies (i.e., by military operating domain or by enabling technology), thereby generating a new framework for better understanding their similarities and differences.

For interested decision makers, we aim to underscore the importance, for both short- and long-term regulation, of forecasting the individual and collective impact of various technologies. A comprehensive account of emerging technologies is needed if effective arms control is to materialise. Our overview of the international stability and human security implications of these technologies – including opportunities – will help to clarify when new arms control approaches are needed. We hope that our study will shed light on whether the international community should regulate these capabilities in the future and how this might best be achieved, helping to ensure that areas of importance are prioritised and limited resources are allocated appropriately. Finally, we hope that our study will give scholars and decision makers a better understanding of expert opinions and a broader perspective on what the future might hold.

This report has four parts. Following this brief introduction, the methods section explains our mixed methods approach to generating, collecting, and analysing the data. The findings section contains the main results of our technology forecasting and ML clustering exercises. This is followed by our conclusions. We encourage the reader to consult the Data Annex to this report (in particular the ‘technology deep dives’ contained therein) and to visit the accompanying webpage ([www.negative-multiplicity.com](http://www.negative-multiplicity.com)), which contains 3D visualisations of our main findings that could not meaningfully be included in a 2D report.

## 2 Methods

This section details our methodological approach. It begins with definitions and then goes on to explain our data collection and analysis. It ends with a critical examination of the limitations of our methodology.

### 2.1 DEFINITIONS

This report evaluates the potential future impact of **emerging technologies**. This term appeared for the first time on the Web of Science in 1969 (Cozzens et al. 2010: 365). For the purpose of our study, we define emerging technologies

**Table 1: Emerging technologies evaluated in this study**

| NO. | TECHNOLOGY CATEGORY                     | EMERGING TECHNOLOGY  |
|-----|---|--|
| 1   | Artificial intelligence                 | AI for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) |
| 2   | Artificial intelligence                 | AI for weapons and effects   |
| 3   | Artificial intelligence                 | AI for cyber operations  |
| 4   | Artificial intelligence                 | AI for information warfare   |
| 5   | Quantum                                 | Quantum for hardening and exploiting systems   |
| 6   | Quantum                                 | Quantum for C4ISR  |
| 7   | Projectiles, propulsions, and platforms | Anti-satellite (ASAT) capabilities   |
| 8   | Projectiles, propulsions, and platforms | Hypersonic weapon systems  |
| 9   | Projectiles, propulsions, and platforms | Directed energy weapons (DEWs)   |
| 10  | Biotechnology and human enhancement     | Physical human enhancement technologies (HET)  |
| 11  | Biotechnology and human enhancement     | Cognitive HET  |
| 12  | Biotechnology and human enhancement     | Synthetic biology  |



as those technologies, scientific discoveries, and technological applications that have not yet reached maturity or are not widely in use but are anticipated to have a major – perhaps disruptive – effect on international peace and security (cf. similarly NATO 2020: 6). In our study, twelve emerging technologies comprised the independent variables in terms of impact.<sup>2</sup> A technology’s impact ultimately depends on the way it is applied and what function(s) it is applied to. Our study focuses specifically on the military applications of emerging technologies. Table 1 lists the twelve emerging technologies in reference to four broader technology categories.<sup>3</sup> Table 2 provides short descriptions of the technologies’ current and/or potential uses.

**Table 2: Current and potential uses of the emerging technologies evaluated in this study**

| NO. | EMERGING TECHNOLOGY        | CURRENT/POTENTIAL USES  |
|-----|----------------------------|---|
| 1   | AI for C4ISR               | AI for C4ISR could enhance clarity and flexibility in combat. Potential uses include intelligence gathering and analysis, early warning, and just-in-time wargaming/simulations that generate AI-recommended courses of action. These processes augment and, in some circumstances, replace human perception and judgement. This technology could also target adversarial systems to spoof sensor data or communications.                       |
| 2   | AI for weapons and effects | AI for weapons and effects can be used to surveil, capture, disable, and/or strike human and material targets. It could generate specific intelligence benefits, including pattern-of-life analysis and decision support for targeting. Such systems could be employed narrowly (e.g., ship-to-ship naval warfare) or in more complex conditions (e.g., urban counterinsurgency).   |
| 3   | AI for cyber operations    | AI can be used to detect, defend against, and facilitate cyberattacks, either independently (i.e., bot vs. bot/bot vs. human) or collaboratively (i.e., a human-machine team). It has the potential to speed up discovery, evaluation, and response processes far beyond human abilities. Specific applications could include advanced vulnerability scanning and exploitation, as well as concealment and false flagging of offensive actions. |

|   |  |  |
|---|--|--|
| 4 | AI for information warfare                   | AI can be utilised to distort and weaponize information in both peace- and wartime, <i>inter alia</i> in the form of ‘deep fakes’ (i.e., synthetic media in which a person in an image or video is either replaced or manipulated). AI can also be used to detect and counter these tactics. AI has the potential to generate a level of contrived realism that surpasses prior techniques used to fake information.                                     |
| 5 | Quantum for hardening and exploiting systems | Quantum technology could provide new and more effective attack vectors and defences in the cyber domain. As an offensive tool, quantum technologies could be used to decrypt data previously secured by public key encryption schemes. Used defensively, quantum-resilient algorithms could offer a new approach to encryption that can withstand even quantum computers. Quantum key distribution could allow for the safe exchange of encryption keys. |
| 6 | Quantum for C4ISR                            | Quantum technology has the potential to significantly improve the C4ISR of multi-domain battlefields. Quantum computing could optimise ML/AI improvement and data analysis, which is critical to surveillance, reconnaissance, and target identification. Quantum imaging offers various applications for, <i>inter alia</i> , quantum radar, 3D cameras, and stealth rangefinders.  |
| 7 | ASAT capabilities <sup>4</sup>               | ASAT capabilities fall into two categories: ground-to-orbit capabilities, which deliver a kinetic or directed-energy effect from Earth to targets, and co-orbital capabilities, which deny or degrade space assets and enable the covert/overt modification of satellites on orbit. In the case of both kinetic and co-orbital ASATs, the damage to the target satellite is often irreversible, as is the increase of space debris in orbit.             |
| 8 | Hypersonic weapon systems                    | Hypersonic weapon systems are capable of exceeding speeds of Mach 5 within the atmosphere. A combination of speed, manoeuvrability, stealth, and ability to evade defensive systems makes hypersonic weapon systems unique. Hypersonic flight vehicles can be used for reconnaissance or to deliver – in swarm or salvo – high-energy kinetic strikes against both standard military and high-value, time-sensitive targets.                             |
| 9 | Directed energy weapons                      | DEWs are ranged weapons that damage targets by exposing them to highly focused energy in the form of a particle beam, a high-energy laser, or microwaves. They may be used against human or material targets or to intercept, disrupt, and destroy autonomous drone swarms, hypersonic missiles, and other emerging weapons technologies that challenge traditional defences in innovative ways.   |

|    |  |  |
|----|--|--|
| 10 | Physical human enhancement technologies  | Physical HET could potentially optimise bodily abilities such as endurance, speed, fitness, muscle strength, infection prevention, wound control, pain reduction, and motor ability via integrated robotics (e.g., exoskeletons or 3D-printed replacement parts), neural interfaces, pharmacological approaches to physical enhancement (e.g., reducing sensitivity to pain), ultralight body armour, new biosensors and bioinformatics, nanotechnologies to monitor and dispense drugs, and genetic manipulation. |
| 11 | Cognitive human enhancement technologies | Cognitive HET could potentially enhance human learning capacities, memory formation, attention, sleep efficiency, and concentration via genetic manipulation, neural interfaces, socio-technical symbiosis with AI or autonomous systems, and pharmacological approaches to increase memory retention, improve situational awareness, and enhance tactical and operational decision making.  |
| 12 | Synthetic biology                        | Synthetic biology involves the deliberate design, engineering, and creation of novel synthetic or modified biological components or systems, based on rapid advances in molecular biology, systems engineering, information science, and other emergent technical fields. This could include new pathogens and novel biological or chemical agents with explicitly engineered and targeted effects such as increased virulence, physical, neurological, or physiological impacts, and genetic susceptibility.      |

We define **international stability** in a narrow sense, with stability reflecting a stable nuclear relationship – historically between the United States and the Soviet Union – that is not prone to crisis instability or arms race pressures (cf. Snyder 1965) and apply this understanding of stability to the U.S.–Russian and U.S.–Chinese nuclear dyads.<sup>5</sup> As opposed to state- or bloc-centred security approaches, we understand **human security** to focus on the individual, putting the safety and security of human beings, and civilians in particular, at the centre of attention (Tadjbakhsh and Chenoy 2006). Human security also relates to regulation aimed at mitigating unnecessary or unjust harm in war (Frei 1988).

To make international stability and human security more analytically accessible, we broke them down into three variables: arms race stability, crisis stability, and humanitarian principles. These comprise the three dependent variables for our study. We define **arms race stability** as the absence of incentives to increase the quantity or quality of a state’s nuclear forces (cf. also Acton 2013:

121; Gray 1980: 144). We define **crisis stability** as the absence of incentives to use nuclear weapons first in a crisis (cf. similarly Acton 2013: 121; for more detail, see Gray 1980: 146).<sup>6</sup> Finally, **humanitarian principles** encompass both moral and legal expectations of appropriate conduct as regards the use of force (cf. Frei 1988). In our understanding, this includes military compliance principles such as distinction, proportionality, precaution, and the prevention of unnecessary suffering. Humanitarian principles thus comprise a canon of lawful conduct in times of war, which originated from The Hague and Geneva Conventions and were further elaborated upon, *inter alia*, in the proceedings of the UN Certain Conventional Weapons Conventions and humanitarian arms control measures following the end of the Cold War (Borrie and Randin 2005).<sup>7</sup>

The relationship between international stability and human security, based on the definitions we have provided, is an interactive one. The possible effects of instability and deterrence failure could be catastrophic, particularly if they lead to nuclear weapon use. The latest simulations have reaffirmed that even a limited, regional nuclear war could kill millions, disrupt the global climate, and lead to mass starvation (Toon et al. 2019). These effects would directly impact the safety and security of millions – if not billions – of human beings. In turn, the (in)security of individuals, and particularly of civilians, can have far-reaching and still under-explored effects on stability between nuclear-armed adversaries. The ongoing war in Ukraine highlights that Russian war crimes committed against civilians can serve as powerful motivations for Western leaders to increase their military support of Ukraine, thereby possibly increasing the risk of a larger conflict between Russia and NATO (The Editorial Board 2022).

## 2.2 DATA COLLECTION

Our methodology falls under the umbrella of futures and foresight methods. Futures and foresight methods encourage the analysis and consideration of a range of future possibilities to inform decision making and public policy (Asselt 2010). According to Kaplan, Skogstad, and Girshick (1950: 93), '[m]any policy decisions require foreknowledge of events which cannot be forecast either by strict causal chains (as can eclipses) or by stable statistical regularities (as can the number of traffic deaths in a given period). For prediction of such events, the policy maker has no recourse but reliance on the judgment of experts.' We

believe that foresighting based on the judgement of experts can help policy-makers to better anticipate the potential impact of technological change and identify when early political action to prevent the most harmful consequences is needed.

Since World War II, researchers have endeavoured to forecast military technology developments that might confer strategic advantages and improve defensive capabilities. More than half a century has passed since the publication of the first technology foresight study. More recently, Kott and Perconti (2018) analysed the accuracy of technology foresight studies conducted in the 1990s with a time horizon of 2020. They assessed the overall accuracy as relatively high, which underlines the practical utility of these studies. However, the authors did notice that forecasting accuracy is greater for technologies with primarily physical effects, whereas accuracy lowers when forecasting technologies whose primary functions are information acquisition and processing. In line with that finding, Armstrong and Sotala (2015) conclude that experts' forecasts on AI progress have historically proved rather ineffectual. This result could speak, in part, to the definitional issues around emerging technologies. O'Hanlon (2000) predicted for the period between 2000–2020 that only two out of 29 technology areas would be expected to bring a revolutionary change, namely computer hardware and computer software. Revisiting his findings, O'Hanlon (2018) noticed that most of his estimates turned out to be correct, notwithstanding a few hyperbolic assumptions. He concluded that the examination of various kinds of literature on technology, in addition to consultation with a variety of experts, is a fruitful approach.

We used a mixed methods approach to collect the data for this study. In the Autumn of 2021, we asked 30 experts<sup>8</sup> whose current and previous work focuses on the intersection of emerging technologies and international/human security to evaluate the twelve selected technologies. The experts completed a so-called technology scoring exercise that was inspired by the RAND-developed Systematic Technology Reconnaissance, Evaluation, and Adoption Methodology (STREAM).<sup>9</sup> STREAM tasks experts with assessing the likely impact of a given technology and the likelihood of its reaching maturity within a specified timeframe.<sup>10</sup> Put differently, the technology scoring exercise evaluated the twelve selected technologies with regard to: 1) their current and forecasted technological maturity levels, and 2) their anticipated impact on international stability and human security.

To evaluate the current and forecasted technology maturity levels, we asked experts to score the technology readiness level (TRL) of the twelve selected technologies in the United States, Russia, and China on a scale from one to nine. We had three objectives in mind: first, to clarify how experts view the current and future technology landscape; second, to clarify how experts view the technology development trajectories of the United States, Russia, and China relative to each other; and third, to provide a foundation for the impact assessment section of the technology scoring exercise. Table 3 illustrates the indicators of technological maturity associated with the nine TRL scores that we provided to experts.

**Table 3: Technology Readiness Level scale and bands**

|             |   |   |           |
|-------------|---|---|-----------|
| RESEARCH    | 1 | Basic principles observed                                 | TIME<br>↓ |
|             | 2 | Technology concept formulated                             |           |
|             | 3 | Experimental proof of concept                             |           |
| DEVELOPMENT | 4 | Technology validated in lab                               |           |
|             | 5 | Technology validated in relevant environment              |           |
|             | 6 | Technology demonstrated in relevant environment           |           |
| DEPLOYMENT  | 7 | System prototype demonstration in operational environment |           |
|             | 8 | System complete and qualified                             |           |
|             | 9 | Actual system proven in operational environment           |           |

The technology scoring exercise began by asking experts to score TRLs in the United States, Russia, and China for the year we conducted our study: 2021. It went on to ask them to forecast TRLs in the three countries for 2030 and 2040 and to describe any barriers to or drivers of the development and/or deployment of these technologies.<sup>11</sup> We then used standard deviation as a proxy to measure the extent to which experts' TRL scores exhibited uniformity or difference.

The technology scoring exercise then shifted its focus to evaluating the potential future impact of the twelve emerging technologies on our three dependent variables. For each technology in the exercise, we asked experts a total of 54 questions, nine of which had multiple choice response options, six of which were open text questions, and 39 of which had both multiple choice and open text response options. We restricted the scope of the questions on arms race and crisis stability to two nuclear dyads – the United States–Russia and the United States–China – anticipating that these dyads will be the most significant for peace and security in the next twenty years and are thus deserving of particular scrutiny. We believe that those two dyads also include the three countries most able to develop and integrate various emerging technologies into their armed forces over the next twenty years. This would have additional potential impacts on the horizontal proliferation of emerging technologies as well as on multilateral non-proliferation efforts. We were also interested in learning whether experts thought that their inimical relationships would act as a potential catalyst for technology development and application in a military context. By contrast, our questions on humanitarian principles comprised all ‘state and non-state actors’.

Thirty-two questions gave experts an opportunity to score both the extent to which these technologies are likely to strengthen or improve arms race stability, crisis stability, and humanitarian principles and the extent to which they are likely to *weaken or deteriorate* these same outcomes. The logic for including both options was that a given emerging technology could have both a positive and a negative impact, depending on its application.

For each question, experts were invited to give an ordinal score between zero (= ‘to no extent’) and five (= ‘to a very high extent’).<sup>12</sup> They were encouraged to score only those technologies they felt confident assessing and to skip any questions that they regarded as irrelevant to a given technology. When conducting expert outreach, we sought out experts who felt comfortable evaluating at least five of the twelve technologies. We also provided the experts with space to explain their qualitative justification for each numerical score or to leave additional comments. Thirty experts completed the technology scoring exercise in total. Table 4 shows a template of the technology scoring exercise for a given technology that we sent to experts, inclusive of all 54 questions.

**Table 4: Technology scoring exercise for a given technology**

| 0 TECHNOLOGY READINESS LEVEL (TRL)  |   |                        |   |
|---|---|------------------------|---|
| <b>Guiding question:</b> What is the technological maturity level of this technology now, and how might this change in the next twenty years?   |   |                        |   |
| <b>Guidance for respondents:</b> TRL refers to the adoption and application of this technology by the armed forces of a given state. Forecasting the anticipated TRL over the next twenty years and any barriers to – or drivers of – its actualisation will help the research team to make sense of how experts evaluate the challenges and opportunities presented by a given technology. |   |                        |   |
| 0.1   | What is the <b>present</b> TRL of this technology?<br><i>(multiple choice)</i>  | For the United States? | For Russia?<br>For China?                                       |
| 0.2   | What is the <b>anticipated</b> TRL of this technology in ten years' time (i.e., 2030)?<br><i>(multiple choice)</i>  | For the United States? | For Russia?<br>For China?                                       |
| 0.3   | What is the <b>anticipated</b> TRL of this technology in twenty years' time (i.e., 2040)?<br><i>(multiple choice)</i>   | For the United States? | For Russia?<br>For China?                                       |
| 0.4   | Please list the main <b>barriers</b> to the application of this technology today:<br><i>(open text entry)</i>   | For the United States? | For Russia?<br>For China?                                       |
| 0.5   | Please list the main <b>drivers</b> of the application of this technology today: <i>(open text entry)</i>   | For the United States? | For Russia?<br>For China?                                       |
| 1 ARMS RACE STABILITY CONSIDERATIONS: THE ABSENCE OF INCENTIVES TO INCREASE THE QUANTITY OR QUALITY OF A STATE'S NUCLEAR FORCES   |   |                        |   |
| <b>Guiding question:</b> What are the arms race stability considerations associated with the application of this technology in a military context?  |   |                        |   |
| <b>Guidance for respondents:</b> The questions in this section relate to arms race stability considerations in two nuclear dyads (the United States and Russia, and the United States and China), as well as multilateral non-proliferation efforts. We define arms race stability as the absence of incentives to increase the quantity or quality of a state's nuclear forces.            |   |                        |   |
| 1.1a  | To what extent could applications of this technology provide the United States with <b>real/perceived military advantages</b> (vis-à-vis Russia)?   | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 1.1b  | To what extent could applications of this technology provide the United States with <b>real/perceived military advantages</b> (vis-à-vis China)?  | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 1.2   | To what extent could this technology affect the <b>military spending priorities</b> of the United States?   | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 1.3a  | To what extent could the proliferation and application of this technology for military purposes by actors other than the United States, Russia, and China <b>positively</b> affect the <b>regional stability</b> of Europe and East Asia? | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |



|   |   |                 |   |
|---|---|-----------------|---|
| 1.3b  | To what extent could the proliferation and application of this technology for military purposes <i>by actors other than</i> the United States, Russia, and China <b>adversely</b> affect the <b>regional stability</b> of Europe and East Asia? | Multiple choice | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 1.4a  | To what extent could this technology <b>positively</b> affect <b>existing arms control agreements</b> between the United States and Russia?   | Multiple choice | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 1.4b  | To what extent could this technology <b>adversely</b> affect <b>existing arms control agreements</b> between the United States and Russia?  | Multiple choice | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 1.5a  | To what extent could this technology <b>positively</b> affect <b>existing multilateral non-proliferation agreements?</b> (e.g., the NPT)  | Multiple choice | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 1.5b  | To what extent could this technology <b>adversely</b> affect <b>existing multilateral non-proliferation agreements?</b> (e.g., the NPT)   | Multiple choice | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 1.6a  | To what extent could this technology <b>positively</b> affect existing <b>bi- or multilateral measures of control?</b> (i.e., verification and monitoring)  | Multiple choice | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 1.6b  | To what extent could this technology <b>adversely</b> affect existing <b>bi- or multilateral measures of control?</b> (i.e., verification and monitoring)   | Multiple choice | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| <i>If there are any important variables that you think we have left out of this section, please note them here:</i> |   |                 |   |

**2 CRISIS STABILITY CONSIDERATIONS: THE ABSENCE OF INCENTIVES TO USE NUCLEAR WEAPONS FIRST IN A CRISIS**

**Guiding question:** What are the crisis stability considerations associated with the application of this technology in a military context?

**Guidance for respondents:** The questions in this section relate to the likelihood of the escalation of an ongoing crisis past the nuclear threshold, in a theoretical crisis situation that includes the United States, Russia, and China. We define crisis stability as the absence of incentives to use nuclear weapons first.

|      |   |                 |   |
|------|---|-----------------|---|
| 2.1  | To what extent could this technology deliver, or enable the delivery of, a <b>disarming first strike</b> ?                  | Multiple choice | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 2.2a | To what extent could this technology be used to <b>improve</b> nuclear command, control, and communications ( <b>NC3</b> )? | Multiple choice | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 2.2b | To what extent could this technology be used to <b>degrade</b> nuclear command, control, and communications ( <b>NC3</b> )? | Multiple choice | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 2.3a | To what extent could this technology <b>increase</b> the <b>availability and quality of information</b> during a crisis?    | Multiple choice | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |

|   |  |                        |   |
|---|--|------------------------|---|
| 2.3b  | To what extent could this technology <b>reduce</b> the <b>availability and quality of information</b> during a crisis?   | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 2.4a  | To what extent could the technology <b>increase</b> <b>decision making time</b> during a crisis?   | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 2.4b  | To what extent could the technology <b>reduce</b> <b>decision making time</b> during a crisis?   | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 2.5a  | To what extent could the technology <b>increase</b> <b>situational awareness</b> during a crisis?  | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 2.5b  | To what extent could the technology <b>reduce</b> <b>situational awareness</b> during a crisis?  | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 2.6   | To what extent could this technology modify a <b>human decision maker's physical, cognitive, or emotional abilities</b> (e.g., via implants, drugs, or genetic modifications)? | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| <i>If there are any important variables that you think we have left out of this section, please note them here:</i> |  |                        |   |

### 3 HUMANITARIAN PRINCIPLES

**Guiding question:** What are the humanitarian considerations associated with the application of this technology in a military context?

**Guidance for respondents:** Humanitarian considerations encompass both moral and legal expectations concerning appropriate conduct as regards the use of force. The questions in this section relate to the use of this technology by and against both state and non-state actors.

|      |   |                        |   |
|------|---|------------------------|---|
| 3.1  | To what extent could this technology <b>challenge existing legal treaties and agreements</b> ?  | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.2a | To what extent could this technology <b>strengthen</b> compliance with the principle of <b>distinction</b> (i.e., between the civilian population and combatants, civilian and military objects, and/or targetable and protected combatants)? | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.2b | To what extent could this technology <b>weaken</b> compliance with the principle of <b>distinction</b> (i.e., between the civilian population and combatants, civilian and military objects, and/or targetable and protected combatants)?     | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.3a | To what extent could this technology <b>strengthen</b> compliance with the principle of <b>proportionality</b> ?  | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |

|      |   |                        |   |
|------|---|------------------------|---|
| 3.3b | To what extent could this technology <b>weaken</b> compliance with the principle of <b>proportionality</b> ?  | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.4a | To what extent could this technology <b>strengthen</b> compliance with the principle of <b>precaution</b> (i.e., precautions taken to avoid, and in any event to minimise, incidental loss of civilian life, injury to civilians, and damage to civilian objects)?              | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.4b | To what extent could this technology <b>weaken</b> compliance with the principle of <b>precaution</b> (i.e., precautions taken to avoid, and in any event to minimise, incidental loss of civilian life, injury to civilians, and damage to civilian objects)?                  | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.5a | To what extent could this technology <b>increase</b> the <b>vulnerability of protected persons</b> in ways not directly related to the principles of distinction, proportionality, or precaution?   | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.5b | To what extent could this technology <b>decrease</b> the <b>vulnerability of protected persons</b> in ways not directly related to the principles of distinction, proportionality, or precaution?   | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.6  | To what extent could this technology subject combatants to harm that might currently be judged as <b>inhumane</b> (i.e., by challenging the rules against superfluous injury and unnecessary suffering, the Martens Clause, and/or other non-legal standards of acceptability)? | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.7a | To what extent could this technology <b>strengthen</b> the ability of actors to exert <b>meaningful human control</b> over targeting decisions by their own forces?   | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.7b | To what extent could this technology <b>weaken</b> the ability of actors to exert <b>meaningful human control</b> over targeting decisions by their own forces?   | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.8a | To what extent could this technology <b>increase</b> <b>accountability</b> challenges (i.e., determining moral and legal liability in the case of weapon misuse/accidental use)?  | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.8b | To what extent could this technology <b>decrease</b> <b>accountability</b> challenges (i.e., determining moral and legal liability in the case of weapon misuse/accidental use)?  | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |
| 3.9a | To what extent could this technology <b>increase</b> <b>attribution</b> challenges (i.e., identifying and laying blame on the perpetrator in the case of a cyber-attack, as well as deception, camouflage, spoofing, and/or information obfuscation)?                           | <i>Multiple choice</i> | In what ways?<br>In which contexts?<br><i>(open text entry)</i> |

|  |                               |  |
|--|-------------------------------|--|
| <p>3.9b To what extent could this technology <b>decrease attribution</b> challenges (i.e., identifying and laying blame on the perpetrator in the case of a cyber-attack, as well as deception, camouflage, spoofing, and/or information obfuscation)?</p> | <p><i>Multiple choice</i></p> | <p>In what ways?<br/>In which contexts?<br/><i>(open text entry)</i></p> |
| <p>3.10a To what extent could this technology <b>raise</b> the threshold/political <b>cost of resorting to war</b> to a degree that makes uses of force <b>less</b> likely?</p>  | <p><i>Multiple choice</i></p> | <p>In what ways?<br/>In which contexts?<br/><i>(open text entry)</i></p> |
| <p>3.10b To what extent could this technology <b>lower</b> the threshold/political <b>cost of resorting to war</b> to a degree that makes uses of force <b>more</b> likely?</p>  | <p><i>Multiple choice</i></p> | <p>In what ways?<br/>In which contexts?<br/><i>(open text entry)</i></p> |
| <p><i>If there are any important variables that you think we have left out of this section, please note them here:</i></p>   |                               |  |

In November 2021, once the technology scoring exercises were complete, we ran four small-group (n<10) exercise debriefs with the experts. The objective of these sessions was to present the preliminary research findings and invite additional qualitative feedback from the experts. The qualitative data from both the technology scoring exercises and the exercise debriefs are synthesised in individual ‘technology deep dives’, which can be found in the Data Annex to this report. The data collection was concluded prior to Russia’s invasion of Ukraine in February 2022.

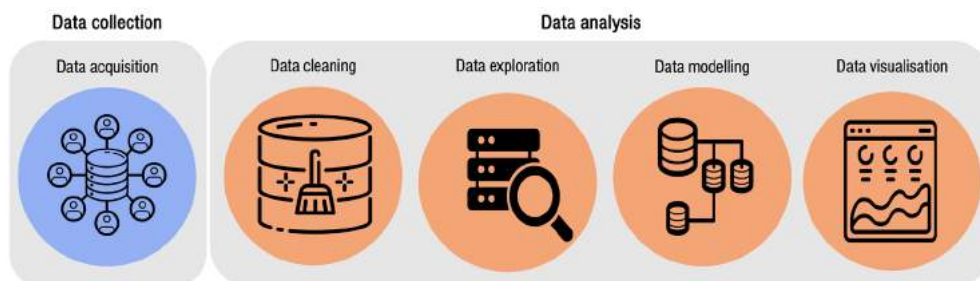
The combination of quantitative and qualitative questions in the technology scoring exercise allowed for the collection of a wide range of data and, ultimately, a more complete assessment. Morgan (2014: 7177) makes the case that ‘there is clear evidence that without some quantification, the use of qualitative words such as “likely” and “unlikely” to describe uncertainty can mask important, often critical, differences between the views of different experts.’

Attached to this report is a Data Annex, which contains the mean impact score per question for each technology and an edited collection of experts’ qualitative remarks (‘technology deep dives’) for each technology. We recommend that it be read in addition to the main report.

## 2.3 DATA ANALYSIS AND VISUALISATION

Once the data was collected, we began a four-step process. In the first step, we scrubbed errors and replaced missing values from our quantitative data to ensure that the data was complete. We then created some preliminary visualisations and ran basic statistics with the objective of better understanding the dataset. These basic statistics included, *inter alia*, question-by-question analysis to see the distribution of scores as well as the mean and median scores for each question. Afterwards, we employed an ML algorithm to identify possible structures in our data. Finally, we visualised the data in a number of figures and tables, which can be found on an accompanying webpage ([www.negative-multiplicity.com](http://www.negative-multiplicity.com)). The webpage contains 3D visualisations of our findings that could not be represented in our 2D report. The orange icons in Figure 1 capture this four-step process.

**Figure 1: Data collection and data analysis pipeline**



The data modelling step warrants closer examination due to our use of an ML algorithm to identify possible structures in our data. ML enables scholars and analysts to identify previously unseen relationships in large datasets. Rather than giving an explicit formula for the distribution of the data, an ML algorithm builds a mathematical model that relies on patterns to infer the structure of the data. In the context of our study, this structure takes the form of technology clusters.

To gain a brief overview of the role of ML in our study, consider the following simplified example. If a hypothetical study examined the impact of one independent variable ( $x$ ) on a dependent variable ( $y$ ), then a data analyst could visualise this data on two axes:  $x$  and  $y$ . This might show a normal distribution

(i.e., a bell curve) or a regression. Determining the ‘shape’ of this hypothetical data is a straightforward task. In comparison, our study has 48 features per technology (i.e., 48 distinct numerical scores given by experts) and twelve technologies. This is a relatively high-dimensional dataset. Putting to one side the qualitative data, an expert who evaluated all the technologies would have given 576 numerical scores in total. Since each of our 30 experts scored at least five of the twelve technologies, we received thousands of individual datapoints. Whereas humans would struggle to recognise possible patterns in the multi-dimensional dataset resulting from our technology scoring exercise, ML is well suited to this task.

We used a clustering algorithm called ‘k-means clustering’ to identify clusters of technologies that experts scored similarly across the scoring criteria. The algorithm groups those technologies that are similar to each other in the same cluster (Al-Masri 2019).<sup>13</sup> Put differently, technologies in the same cluster were determined by the 30 experts to have similar degrees and similar types of effect on arms race stability, crisis stability, and humanitarian principles. Finally, we attempted to validate our findings using statistical methods. In the validation phase, we sought confirmation that the technology clusters identified in the data come from actual differences in the characteristics of the technologies, rather than random chance. We used two validation techniques – ‘Silhouette scores’ and ‘Calinski-Harabasz scores’ – to test the robustness of the technology clusters.<sup>14</sup>

## 2.4 LIMITATIONS

In this section, we discuss a few methodological trade-offs relating to our study and provide justifications for our respective choices.

First, we recognise that expert elicitation methods have several limitations. Tetlock (2017) argues that issue-specific experts are generally poor at forecasting future events, including political phenomena. Humans also unconsciously use a variety of cognitive heuristics, which may undermine our ability to make unbiased probabilistic judgements. Two of the most relevant heuristics in the context of expert elicitation are ‘availability’ and ‘anchoring and adjustment’ (Morgan 2014; Tversky and Kahneman 1974).

‘Availability’ refers to the tendency to assess the probability of an event in terms of the ease with which instances or occurrences can be recalled. Humans tend to ascribe outsized importance to information that comes to mind quickly, rather than considering all relevant information when forecasting future outcomes. Given that the study took place in the middle of the COVID-19 pandemic in 2021, the ‘availability’ heuristic may help to explain experts’ scoring of synthetic biology technologies used to create new pathogens or novel biological or chemical agents, although this is speculation. ‘Anchoring and adjustment’ refers to the phenomenon wherein an individual’s decision is influenced by a particular reference point, or ‘anchor’. This heuristic might help to explain why experts suggested that all twelve technologies are likely to be fully operational by 2040. This prediction could be informed by our decision to establish 2040 as an artificial end point for the technology maturity horizon. Finally, individuals, including experts, may overestimate their knowledge and/or certainty of their responses.<sup>15</sup>

Notwithstanding these shortcomings, we decided in favour of an expert elicitation method because it was our intention to clarify the expert view, with all its limitations and biases.<sup>16</sup> In addition, publicly available data on the impact of emerging military technologies is still very rare. Thus, generating data by surveying international experts may help to fill a gap in the research.

Second, we used existing professional networks to identify possible participants for this study. We recognise that – like any non-random sampling method – this did not result in a representative sample and that the approach lends itself to community bias risk (cf. Bonaccorsi, Aprea, and Fantoni 2020). In defence of this approach, we might appeal to the specific scholarly and professional backgrounds of our experts, who are specialists in the intersection of emerging technologies and international security policies. Perhaps more problematic is the fact that all the experts included in this study were based in Western Europe and North America. With this acknowledged, our framework lends itself to broadening the analysis in future scholarly work. Accordingly, our study should be seen as a first step. Future work can and should build on our study to incorporate Russian, Chinese, and other perspectives.

Third, ours is a high-dimensionality dataset, which means that the dataset has more features than data points. In our study, there are more questions in the technology scoring exercise (i.e., 48 features) than there are technologies

(i.e., twelve data points). The so-called ‘curse of dimensionality’ is a well-known problem in clustering algorithms (Steinbach, Ertöz, and Kumar 2004: 11–14). It arises because the distances between individual datapoints become increasingly uniform as the number of dimensions in the data increases relative to the number of data points. There is no clear definition or threshold value above which the curse of dimensionality occurs or becomes problematic. Nevertheless, we calculated the pairwise distances between data points to assess whether these distances were approaching the same value.<sup>17</sup> We then plotted these pairwise distances on a histogram, which returned a bimodal distribution. This, among other metrics, gave us confidence that our technology clusters were robust and meaningful.

Finally, we concede that unsupervised ML involves a significant amount of trial and error, for example when deciding on the most appropriate number of clusters. We validated the number of clusters by using additional validation techniques, such as Silhouette and Calinski-Harabasz scores, which nevertheless produce approximations. We also recognise that the clustering algorithm does not explain why certain technologies are clustered together; to that end, we used experts’ qualitative remarks.



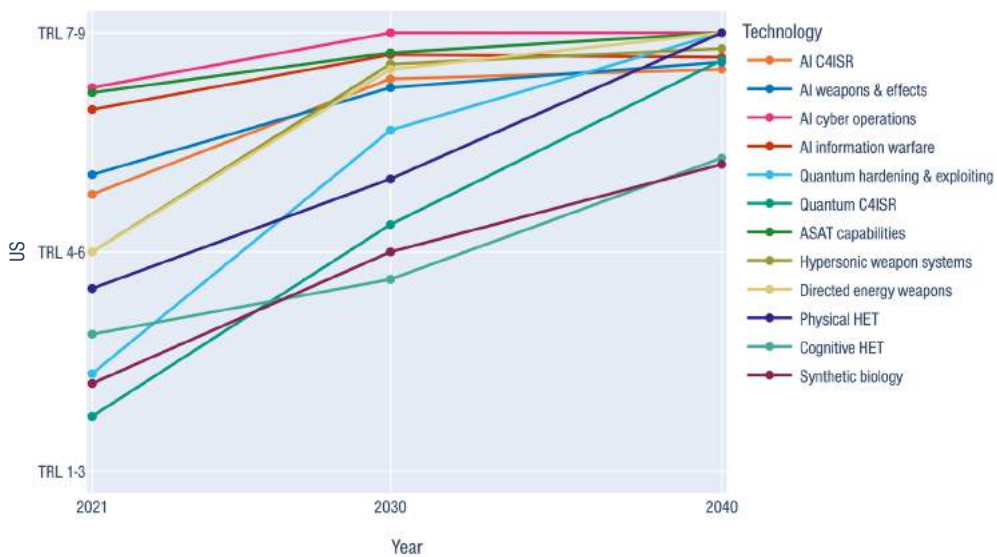
## 3 Findings

This section contains the main findings derived from the technology forecasting and scoring exercises and the ML-derived formulation of technology clusters.

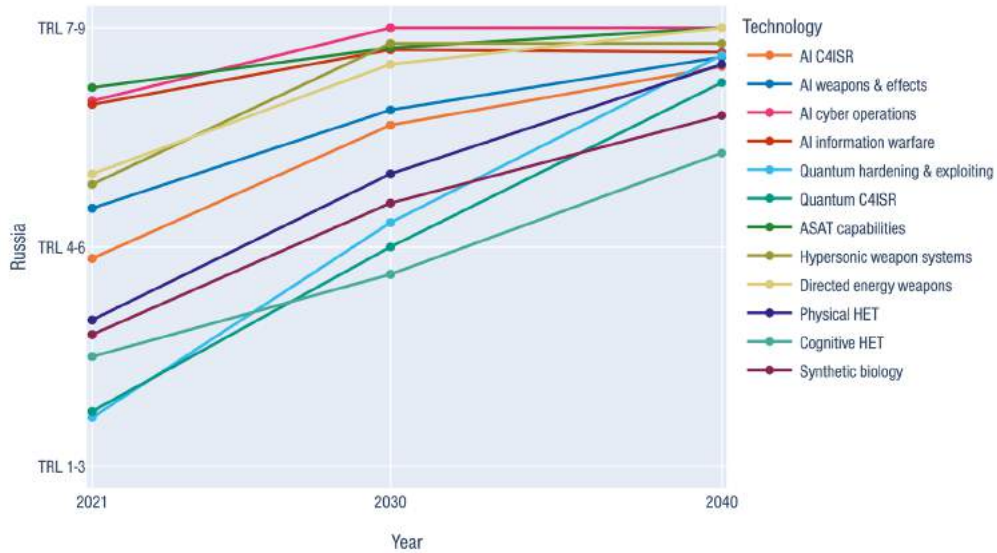
### 3.1 TECHNOLOGY FORECASTING

When forecasting the TRL of the twelve technologies for the United States, Russia, and China, experts anticipated significant variance between the different technologies by 2030. By 2040, however, they expect that most of these technologies will be deployable in an operational environment for all three countries. Figures 2, 3, and 4 illustrate the current (2021) and projected (2030 and 2040) TRLs for all technologies for the United States, Russia, and China, respectively. Each coloured line represents an emerging technology, with time on the x-axis and the nine TRL scores on the y-axis.

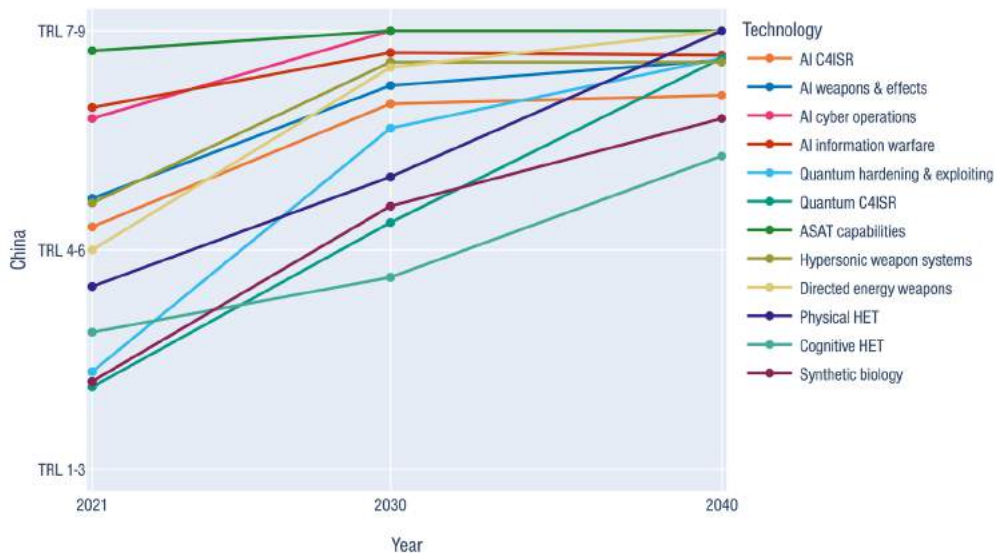
**Figure 2: Current and future TRL for all technologies for the United States**



**Figure 3: Current and future TRL for all technologies for Russia**



**Figure 4: Current and future TRL for all technologies for China**

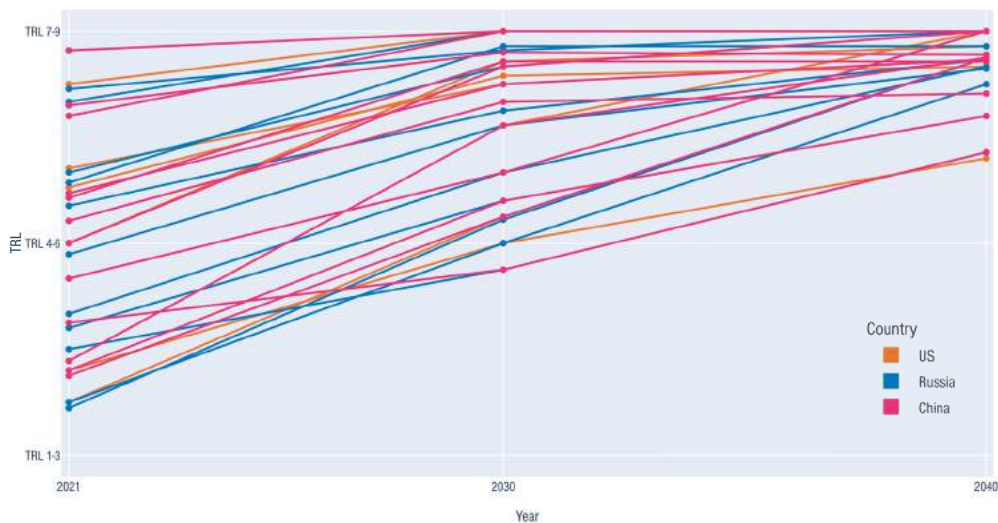


As Figures 2-4 indicate, experts foresaw all technologies moving in the same direction and reaching operational deployability by 2040 in all three countries. They anticipated that some technologies would make significant leaps from a low TRL to a high TRL between now and 2040 (e.g., quantum for C4ISR). On the other hand, some technologies are presently categorised in the TRL 7-9 band, suggesting that they have less maturing to do between now and 2040 (e.g.,

AI for cyber operations). Some technologies were expected to develop rapidly between now and 2030 and less so between 2030 and 2040 (e.g., quantum for hardening and exploiting systems). Other technologies were expected to do the opposite, that is, develop comparatively slowly between now and 2030 and much more rapidly between 2030 and 2040 (e.g., cognitive human enhancement technologies).

Figure 5 overlays the TRLs for each technology and each country. The United States is shown in orange, Russia in blue, and China in pink. Although this graphic is not as intuitive as the others, the take-away message is that experts viewed these three countries as rather evenly matched in their technology development trajectories.

**Figure 5: Overlaying the current and future TRL for all countries**



There is one particularly interesting insight that comes from Figure 5: whereas the 2040 axis exhibits expert consensus that most of the emerging technologies will have reached operational deployability by this point, experts anticipated that only half of the technologies surveyed in our study will be deployable by 2030. Among the latter, they expected that hypersonic weapon systems, directed energy weapons, and militarised quantum applications will undergo rapid maturation between now and 2030.

Applying standard deviation to gauge agreement and disagreement among experts' TRL scores, we found that, for almost all of the technologies, experts exhibited more disagreement around present TRLs than future ones. Figure 6 shows the twelve emerging technologies on the x-axis and standard deviation on the y-axis. A shorter bar signifies less deviation from the mean and thus greater agreement among experts on TRL scores for a given technology across all three countries. In the case of AI cyber operations, there is no bar at all for the 2030 and 2040 axes because there is no deviation from the mean TRL score for these years.

**Figure 6: Mean TRL standard deviation across all three countries**

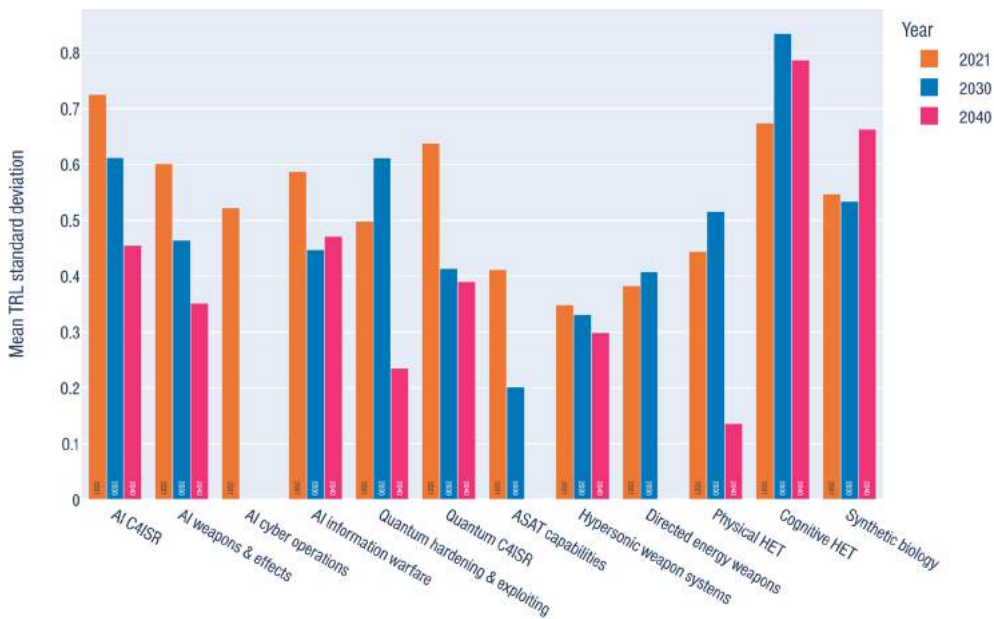
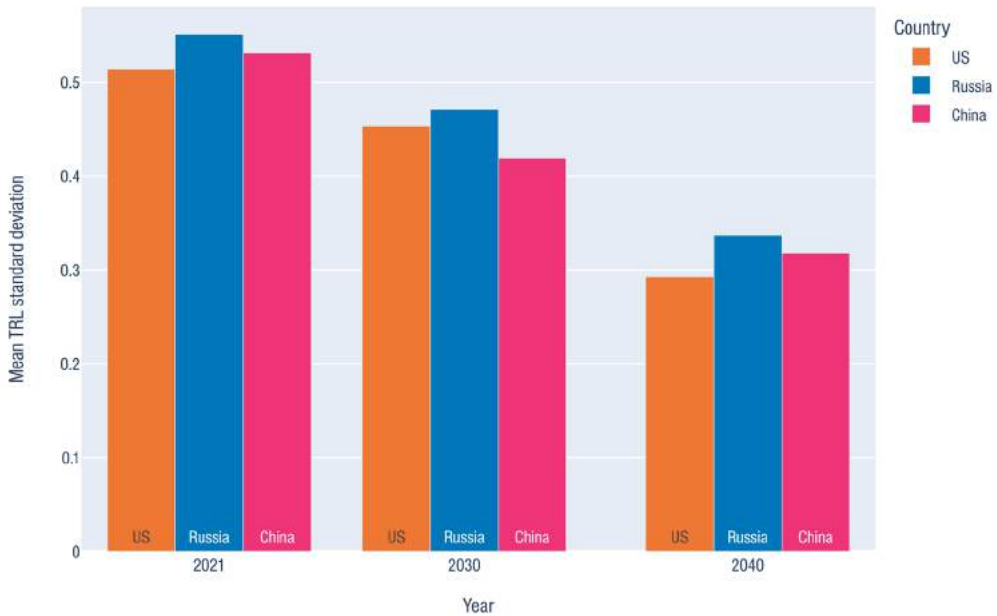


Figure 7 shows another metric for expert (dis)agreement: the x-axis represents the time horizon, and the y-axis represents the mean TRL standard deviation across all technologies. As before, the United States is shown in orange, Russia in blue, and China in pink. This graph shows that experts exhibited most disagreement vis-à-vis Russia's TRL scores, but not by a significant margin. In the qualitative remarks in the scoring exercise, some experts mentioned that Russia faces comparatively greater barriers to developing and deploying some of these technologies due to high levels of corruption, a static innovation system, a less developed private sector, a relative lack of economic resources, and lack of access to international collaboration. It is important to reiterate that these responses were given prior to Russia's February 2022 invasion of Ukraine.

**Figure 7: Mean TRL standard deviation across all technologies**



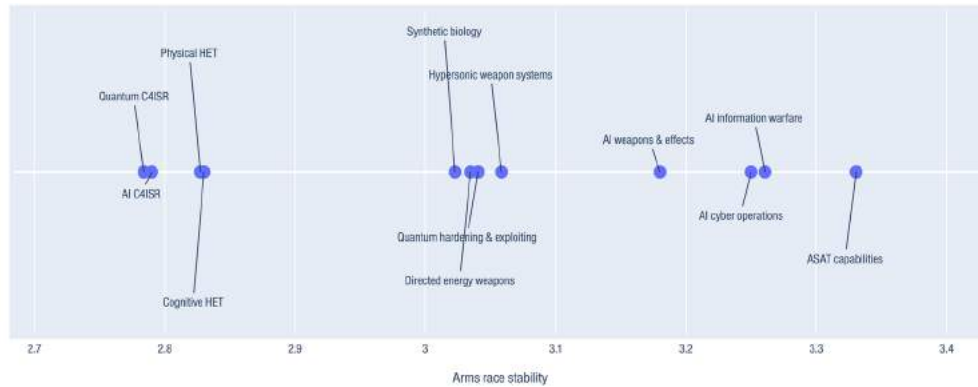
### 3.2 TECHNOLOGY IMPACT ASSESSMENT

The technology scoring exercise established a baseline of current and projected TRLs for the twelve emerging technologies and produced several findings regarding their potential impact on arms race stability, crisis stability, and humanitarian principles. This section explores the constituent technologies, the ML-derived technology clusters, and the anticipated impact of each technology cluster over time.

#### 3.2.1 TECHNOLOGIES' INDIVIDUAL IMPACT

Figures 8–10 show the relative position of each emerging technology on the arms race stability, crisis stability, and humanitarian principles axes. The higher the value, the more negative the expected impact.

As Figure 8 indicates, experts anticipated that ASAT capabilities and AI-enabled military applications (except for C4ISR purposes) would have the most negative impact on arms racing in the coming two decades of all the technologies surveyed in this study. In their qualitative comments, they clarified that due

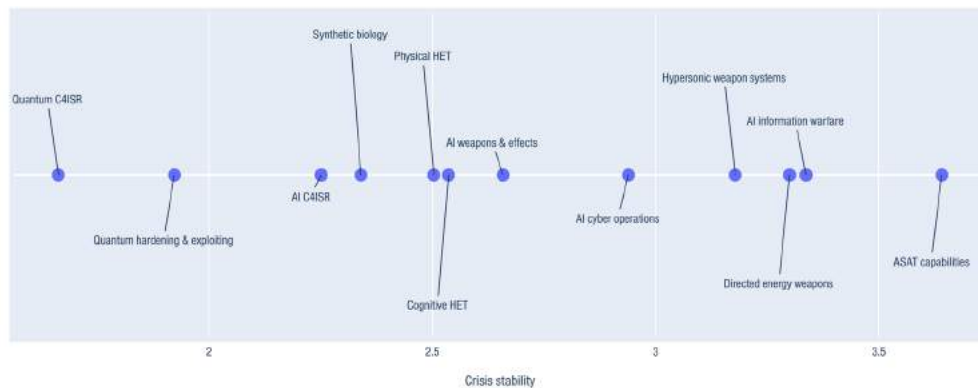
**Figure 8: Emerging technologies' impact on arms race stability**

to the increasing proliferation of satellites and **ASAT capabilities**, they expect that the United States, Russia, and China will perceive a need to deter or defeat hostile activities in space. They also noted the symbolic value of ASATs as a driver of proliferation (i.e., testing or demonstrating ASAT capabilities signals a readiness for space warfare). Experts noted that the United States is particularly motivated by an ambition to maintain space supremacy. In turn, disrupting U.S. access to space and space-enabled data and services was seen by experts as creating significant military gains for China and Russia. Experts also mentioned concerns that ASAT capability development by nuclear possessors other than the United States, Russia, and China could deepen the divide between nuclear and non-nuclear weapon states, with adverse effects on multilateral agreements like the Treaty on the Non-Proliferation of Nuclear Weapons (NPT).

As regards AI-enabled military applications (except for C4ISR purposes), experts highlighted Russia's particular interest in developing **AI for information warfare** due to the comparably lower price tag of this technology and its role in Russia's sub-threshold warfare doctrine. Experts also mentioned the negative effects of this technology application on negotiating and/or upholding arms control agreements in an environment of distrust, as well as its adverse impact on verification and monitoring. Regarding **AI-enabled cyber operations**, experts foresaw an increase in financial and technical investments by the United States, Russia, and China and cautioned that AI cyber operations will likely lead to more complex and destructive covert activities, thereby intensifying competition in cyberspace. The current lack of non-legally binding regulation in this area was cited as an additional source of negative pressure on arms race stability. Experts anticipate that **AI-incorporated weapons and effects** will affect

arms race stability due, in part, to an increase in U.S. funding of these systems. According to the experts, much of this spending is driven by the (not necessarily accurate) perception that AI-incorporated weapons systems will outperform their human counterparts on the battlefield. Finally, experts made reference to the competitive geopolitical landscape as a potential driver.

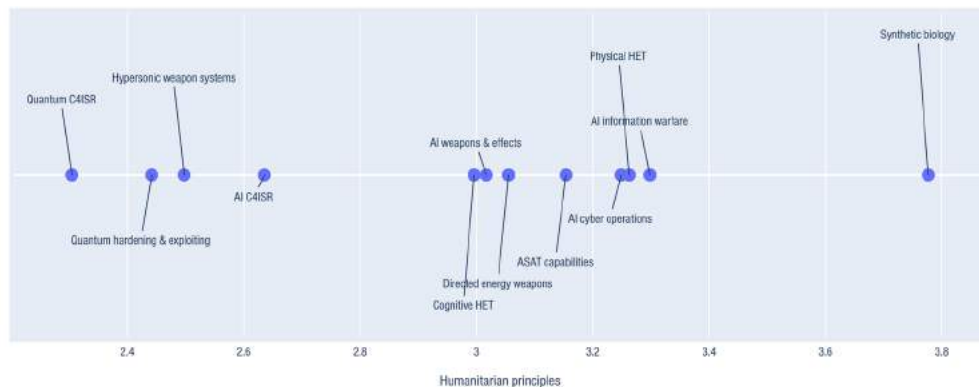
**Figure 9: Emerging technologies' impact on crisis stability**



ASAT capabilities, AI information warfare, DEWs, and hypersonic weapon systems rank highest in terms of their expected potential to destabilise an ongoing crisis, as illustrated in Figure 9. In the qualitative comments, experts highlighted that **ASAT capabilities** employed to deny or disrupt intelligence, surveillance, and reconnaissance (ISR) systems, NC3 satellites, and/or orbital early warning systems could be part of a broader campaign to blind an enemy to an inbound attack. In a crisis, this could trigger conventional and/or nuclear strikes. Experts further cautioned that states might believe that striking an adversary's space-based assets could provide them with a military advantage in a first-strike scenario. Regarding **AI for information warfare**, experts noted that it is more likely that this technology would be used in combination with a kinetic strike or cyberattack than as a stand-alone measure. Further, experts feared that the compound effect of sustained AI-enabled information operations could create divides among national security staffers with regard to threat perception, including what kinds of information they find credible. They also warned that this technology application could destabilise public opinion and put pressure on decision makers to act more quickly in a crisis. Experts suggested that **Directed Energy Weapons (DEW)** could affect crisis stability if states use them defensively to destroy adversary missiles or offensively to

damage or degrade satellites or ‘soak up’ retaliation following a kinetic first strike. Many experts discussed this technology’s ability to degrade NC3 and ISR, noting that DEWs could ‘blind’ or destroy sensors, early warning systems, and space-based communication links. According to the experts, **hypersonic weapon systems** constitute ideal systems for destroying, damaging, or degrading NC3 deep inside enemy territory, which could undermine the target’s ability to retaliate. They also warned that ambiguity regarding the weapons’ intended targets and their payloads (i.e., conventional or nuclear) could intensify instability and incentivise crisis escalation. Finally, experts referred to the ‘use it or lose it’ dynamic potentially created by hypersonic weapon systems, which could lower the threshold for initiating war and create first-mover advantages.

**Figure 10: Emerging technologies’ impact on humanitarian principles**



As visualised in Figure 10, experts predicted that **synthetic biology** would have the most negative impact on humanitarian principles over the next twenty years, by a wide margin. In their qualitative remarks, experts pointed out that biological weapons – particularly those that depend on contagiousness or transmissibility – would lack the capacity to discriminate between legal and illegal human targets in a military context. The difficulty of controlling the spread of such agents was expected to exacerbate civilian vulnerability and harm in both military and non-military settings. Experts also warned that it would likely be difficult to determine the party responsible for releasing a synthetically created pathogen.

Seven technologies occupy a densely populated middle ground in terms of their expected negative impact on humanitarian principles. Here, experts raised several concerns in their qualitative remarks. With regard to **AI for information**



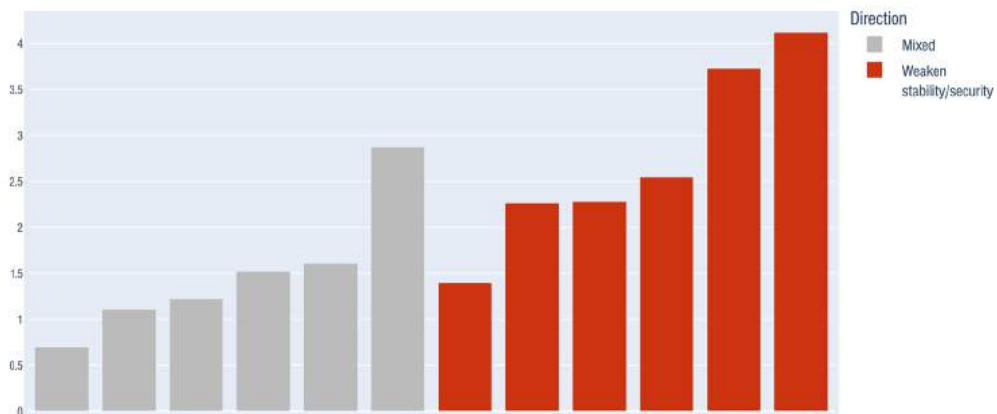
**warfare**, experts concluded that this technology would blur the distinction between civilians and combatants and exploit existing social biases and stereotypes in civilian groups, which could increase the vulnerability of protected persons. On **physical and cognitive HET**, experts highlighted, among other concerns, the possibility that new divisions could open up on the battlefield between enhanced and un-enhanced humans, putting pressure on a range of moral and legal assumptions related to inhumane treatment, prisoner of war status, and accountability. Regarding **AI for cyber operations**, experts noted the difficulty of discriminating between military and non-military objects and expressed concerns about accountability and attribution. For **ASAT capabilities**, experts warned of the profound and indiscriminate second-order effects of ASAT use, such as the potential disruption of critical national infrastructure, the economy, and the internet (of things). With regard to **DEWs**, experts expressed humanitarian concerns, particularly in situations where civilians are present (e.g., for crowd control or reversible electronic attacks on civilian vehicles). Experts anticipated that **AI for weapons and effects** will generate significant challenges for the principle of discrimination, citing the problem of potentially incomplete, inadequate, and flawed targeting data as well as AI biases against certain ethnicities and/or genders. Additional expert concerns related to the erosion of battlefield accountability, a loss of meaningful human control over key military decisions, and the alleged ‘inhumanity’ of autonomously executed lethal strikes.

When evaluating the likely impact of these technologies, experts were given the opportunity to specify whether and in what ways a given technology could strengthen international stability and human security. Thus, we phrased most of the questions in the scoring exercise in both positive and negative terms.

Experts firstly agreed that all of the twelve technologies will weaken at a minimum one of the three dependent variables. Second, experts assessed that six of the technologies (i.e., AI weapons and effects, AI cyber operations, hypersonic weapon systems, directed energy weapons, AI information warfare, and ASAT capabilities) have weakening effects on all three dependent variables. Third, only two technologies (i.e., AI for C4ISR and quantum for C4ISR) show more of a strengthening than a weakening effect on two of three axes. In Figure 11, the y-axis shows the difference between the average strengthening and weakening scores for each technology. The taller the bar, the greater the difference between a given technology’s average strengthening and weakening

scores. Red bars correspond to technologies that experts assessed as having a weakening effect that is greater than their strengthening effect across all three axes. Grey bars correspond to technologies for which the average strengthening score is greater than the average weakening score on at least one axis.

**Figure 11: The extent to which each technology might weaken stability and security, across all three axes**



Of all the technologies, experts scored **AI for C4ISR** as the most ‘neutral’, since its average strengthening and weakening scores are not greatly dissimilar across all three axes. In comparison, **ASAT capabilities** have the largest distance between the average strengthening and weakening scores, meaning that ASAT capabilities were assessed as the most problematic of the technologies and the least likely to strengthen international stability and human security. Table 5 lists the twelve technologies’ individual strengthening and weakening effects on each axis, based on the quantitative scores.

The potentially positive effects of **AI and quantum for C4ISR** purposes are notable. In the qualitative sections of the scoring exercise, experts commented that AI for C4ISR could improve system-wide visibility and analysis, as well as interoperability between platforms, services, and allies. This increase in clarity, they suggested, could mitigate the risk of inadvertent escalation in a crisis. On quantum for C4ISR, experts agreed that the technology would improve the overall information landscape – even in denied or degraded environments – because it would make more information available, process information quicker, and increase confidence in that information. Taken together, these applications could enhance transparency and situational awareness.

**Table 5: Strengthening/weakening effects of each technology, on each axis**

| TECHNOLOGY                                   | ARMS RACE STABILITY | CRISIS STABILITY | HUMANITARIAN PRINCIPLES | OVERALL RESULT |
|--|---------------------|------------------|-------------------------|----------------|
| AI for C4ISR                                 | Strengthen          | Strengthen       | Weaken                  | Mixed          |
| AI for weapons and effects                   | Weaken              | Weaken           | Weaken                  | Weaken         |
| AI for cyber operations                      | Weaken              | Weaken           | Weaken                  | Weaken         |
| AI for information warfare                   | Weaken              | Weaken           | Weaken                  | Weaken         |
| Quantum for hardening and exploiting systems | Weaken              | Strengthen       | Weaken                  | Mixed          |
| Quantum for C4ISR                            | Weaken              | Strengthen       | Strengthen              | Mixed          |
| ASAT capabilities                            | Weaken              | Weaken           | Weaken                  | Weaken         |
| Hypersonic weapon systems                    | Weaken              | Weaken           | Weaken                  | Weaken         |
| DEWs   | Weaken              | Weaken           | Weaken                  | Weaken         |
| Physical HET                                 | Weaken              | Strengthen       | Weaken                  | Mixed          |
| Cognitive HET                                | Weaken              | Strengthen       | Weaken                  | Mixed          |
| Synthetic biology                            | Weaken              | Strengthen       | Weaken                  | Mixed          |

As discussed in the methods section, a likely consequence of the Western- and Anglo-centric composition of our expert pool was that many of those effects deemed positive by experts were expected to strengthen stability by means of exclusively strengthening U.S. and/or U.S. allies' military capabilities vis-à-vis regional competitors. This relates back to underlying assumptions about the potentially stabilising or destabilising effects of symmetrical and asymmetrical technology development and maturity levels among great powers and the related effects on the distribution of power. Further gauging these assumptions would require additional research, which could help to gain a more complete understanding of experts' perceptions. For more information on qualitative expert feedback on the individual technologies, including references to the potentially positive effects of U.S. adversaries 'catching up' on technology development, please refer to the 'technology deep dives' in the Data Annex to this report.

### 3.2.2 TECHNOLOGY CLUSTERS

We used ML to identify similarities and differences in how experts evaluated the impact of the twelve emerging technologies. This resulted in five technology clusters, in which technologies are grouped according to their expected stability and humanitarian impact rather than their technical characteristics.<sup>18</sup> Table 6 lists the five clusters and their expected impact on the three dependent variables. Each technology cluster comprises emerging technologies that were scored similarly by experts across the three dependent variables. The higher the value, the greater the expectation that a given technology will negatively affect or weaken arms race stability, crisis stability, and/or humanitarian principles. Accordingly, ‘high impact’ in Table 6 has a clearly negative connotation.

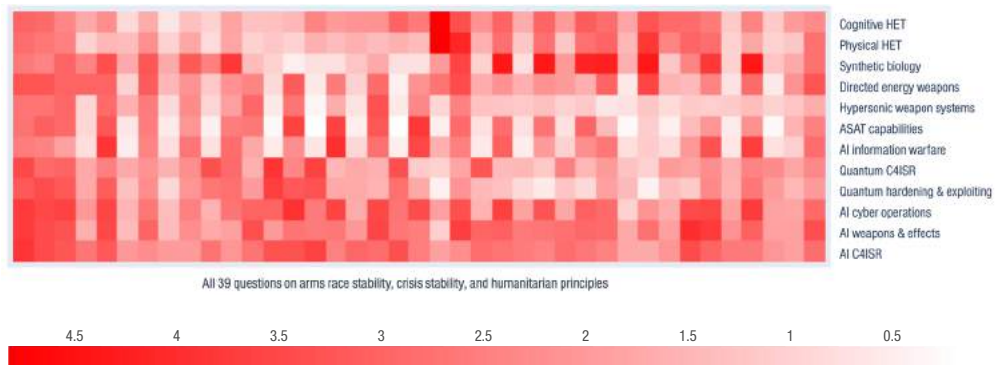
**Table 6: Impact of the five technology clusters**

|           | NAME                               | EMERGING TECHNOLOGIES  | IMPACT ON ...       |                  |                         |
|-----------|------------------------------------|--|---------------------|------------------|-------------------------|
|           |                                    |  | ARMS RACE STABILITY | CRISIS STABILITY | HUMANITARIAN PRINCIPLES |
| CLUSTER 1 | Kinetic/<br>non-kinetic<br>warfare | <ul style="list-style-type: none"> <li>- AI for information warfare</li> <li>- ASAT capabilities</li> <li>- DEWs</li> <li>- Hypersonic weapon systems</li> </ul> | Mid-high            | High             | Mid                     |
| CLUSTER 2 | Militarised AI                     | <ul style="list-style-type: none"> <li>- AI for cyber operations</li> <li>- AI for weapons and effects</li> <li>- AI for C4ISR</li> </ul>                        | Low-high            | Mid              | Low-mid                 |
| CLUSTER 3 | Human enhancement                  | <ul style="list-style-type: none"> <li>- Physical HET</li> <li>- Cognitive HET</li> </ul>  | Low                 | Mid              | Mid-high                |
| CLUSTER 4 | Militarised quantum                | <ul style="list-style-type: none"> <li>- Quantum for hardening and exploiting</li> <li>- Quantum for C4ISR</li> </ul>  | Low-mid             | Low              | Low                     |
| CLUSTER 5 | Weaponised biotechnology           | <ul style="list-style-type: none"> <li>- Synthetic biology</li> </ul>  | Mid                 | Low-mid          | High                    |

Cluster 1 (kinetic/non-kinetic warfare) is of greatest concern among experts, particularly as regards the cluster’s potential impact on arms race and crisis stability. Meanwhile, Cluster 3 (human enhancement technologies) and Cluster 5 (weaponised biotechnology) are of greatest concern among experts in terms of their negative impact on humanitarian principles.

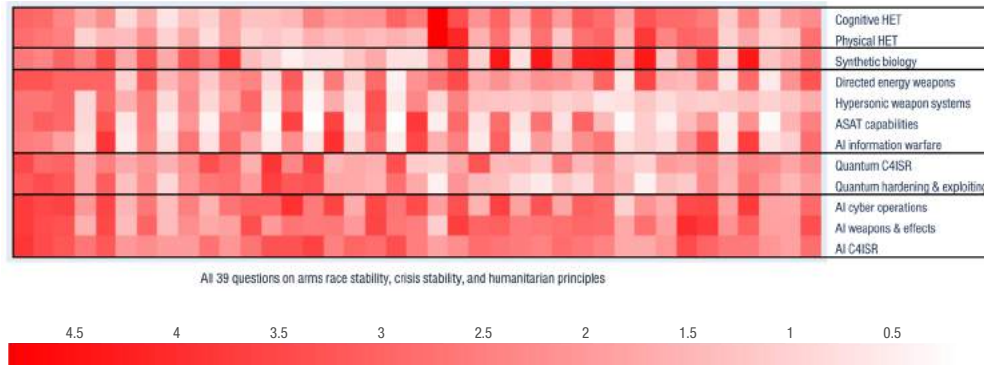
As discussed in the previous section, there are drawbacks to using ML, such as the lack of transparency in clustering. The mechanics of the clustering algorithm might diverge from the reasons a human might give for grouping two alike things together. Figure 12 shows a so-called ‘heatmap’. Along the x-axis are the various technology impact questions that we asked the experts. Moving from left to right, we begin with arms race stability questions, proceed to crisis stability questions, and end with questions pertaining to humanitarian principles. The technologies along the y-axis are grouped by cluster. The darker the square, the higher the average score for the respective question. With this information, some patterns become visible from the data.

**Figure 12: Heatmap of all questions and all twelve technologies**



In Figure 13, a box partitions each cluster to show that the emerging technologies in that cluster were scored similarly. We call these ‘impact passages’. Within each impact passage, vertical bars of similar colours (i.e., all light or all dark) indicate that experts scored technologies similarly for a given question. This exercise resembles the way the computer analyses data: it finds similar scores for a given question and then clusters technologies that share the highest number of similar scores.

**Figure 13: Heatmap with clusters overlaid**

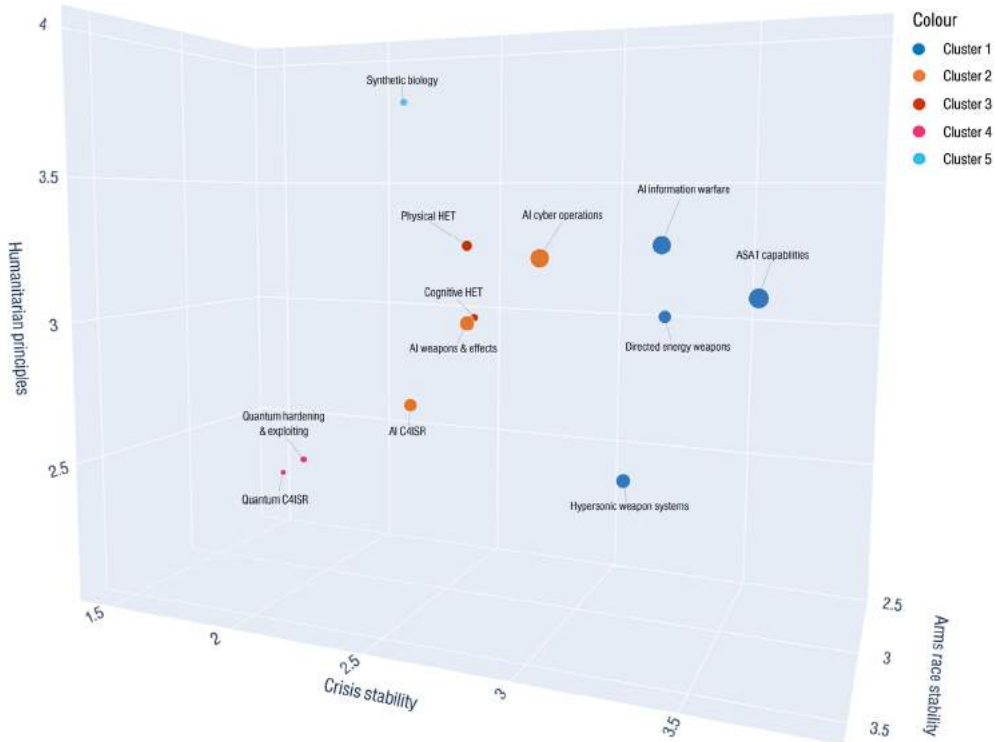


Cluster 1, which includes AI information warfare, ASAT capabilities, directed energy weapons, and hypersonic weapon systems, illustrates most clearly the insights that the heatmap offers. This cluster demonstrates a remarkable amount of cohesion in the way experts scored the constituent technologies. This is notable because, of the five technology clusters, this one constitutes the most diverse group of technologies.

### 3.2.3 ACUTENESS

Once we had used ML to identify five clusters and their potential impact, we considered when the impact of the various technologies was likely to become most acute. Put differently, we wanted to know on what timeline high-impact technologies might become deployable and thus ready for use in a military context. To illustrate this, we combined the impact results from the scoring exercise with the TRLs. As previously mentioned, experts anticipate that most of the twelve technologies will be deployable in an operational environment by 2040. Thus, the more interesting years are 2021 and 2030. Figures 14 and 15 show all twelve technologies in a three-dimensional impact graph, one for 2021 and one for 2030. The three axes correspond to the three dependent variables. Each technology is represented by a dot, which comes in the colours of the respective cluster to which each technology belongs. The larger the dot, the higher the TRL for a given year (2021 and 2030).

**Figure 14: Technology clusters with TRL overlaid for 2021**



For 2021, the experts indicated that three high-impact technologies showed the highest level of deployability: ASAT capabilities, AI for information warfare, and AI for cyber operations. As mentioned above, experts explained the high level of deployability of **ASAT capabilities** in their qualitative comments by referring to the growing proliferation of state- and commercially owned satellites and the parallel military competition between the United States, Russia, and China, including in space. Regarding **AI for information warfare**, experts identified Russia as the main driver and anticipated that the United States will primarily invest in counter-influence AI measures to minimise the risks that information operations could pose. Further, experts clarified that there has been significant interest and corresponding investment in **AI for cyber operations** in the United States, Russia, and China, driven mainly by human limitations in this area and the potential of this technology to strengthen both offensive and defensive operations.

**Figure 15: Technology clusters with TRL overlaid for 2030**

According to experts' estimates, by 2030, **DEWs** and hypersonic weapon systems will join the ranks of high-impact technologies with the highest level of deployability. In the qualitative comments, experts explained the high level of deployability of DEWs by reference to their potentially prominent role in missile defence and anti-satellite capabilities. They also referred to the defensive potential of this technology for countering rockets, artillery, mortars, **hypersonic weapon systems**, and (swarms of) unmanned aerial systems. Regarding hypersonic weapon systems, experts cited the exclusivity of this capability, the political prestige it confers, and perceived first-mover advantages as motivating the United States, Russia, and China to engage in an intensifying race to develop and field this technology. Experts added U.S. missile defence and military competition between China and the United States in the Indo-Pacific region as additional explanations.



## 4 Conclusions

This section highlights our conclusions and points decision makers and scholars towards a number of major concerns about the future impact of emerging technologies.

Our study reveals a combined effect that we term ‘negative multiplicity’.<sup>19</sup> **Negative multiplicity reflects the predominantly negative, concurrent, and in some cases similar, first- and second-order effects that emerging technologies are expected to have on international stability and human security.** Although we gave experts the opportunity to highlight the potentially positive effects of emerging technologies, they anticipated that all technologies will weaken either international stability or human security, and sometimes both. In addition, our study finds that concerns about emerging technologies’ anticipated negative effects are not necessarily limited to one area. Instead, for half of the technologies surveyed, their multi-dimensional negative effects on arms race and crisis stability and on humanitarian principles are expected to become evident over the coming two decades. Taken together, **the net impact of all twelve emerging technologies is negative.** These results confirm the already widespread concern among scholars and decision makers about the anticipated negative effects of certain emerging technologies (cf. Boulanin 2019; Chyba 2020; Favaro 2021; Saalman 2019; Sauer 2021; Sechser, Narang, and Talmadge 2019; Williams 2019). However, our results go further and point to **an entire generation of concerning new technologies, expected to be deployable in a military context by 2040.**

Negative multiplicity, beyond the negative net assessment, has a second dimension. The ML algorithm we used to cluster the technologies revealed a particularly striking result: **impact similarities do not necessarily mirror technological similarities.** The most impactful technology cluster, for example, includes technologies that share few, if any, technical characteristics (i.e., ASAT capabilities, AI for information warfare, DEWs, and hypersonic weapon systems). These technologies are emerging in parallel, meaning that their impact on international stability and human security could be simultaneous, interactive, and non-linear. Our experts’ qualitative comments confirmed that there are likely to be circumstances where these technologies are used in combination to create new effects or to intensify existing ones. Both eventualities deserve further research and could be studied using scenario-building or

tabletop exercises that combine the effects of various technologies in specific crisis situations and as regards human security.

The impact of individual technologies is varied, with some technologies having a more pronounced negative impact than others. Two technologies deserve closer observation here. Our study underscores that **ASAT capabilities show uniquely negative characteristics** across all three dependent variables, but especially on arms race and crisis stability. ASAT capabilities could destabilise nuclear relationships (e.g., by targeting NC3) while also having a severe humanitarian effect through disruptions to civilian services. This disruption could range from satellite-reliant infrastructure like IoT devices to online banking, positioning systems, or self-driving cars. These concerns are worth highlighting given the ongoing proliferation of commercial and state-owned satellites and the increasing reliance of various civilian and military services on space-based assets, including in the communications and information realms. **Equally concerning is the expected negative impact of AI for information warfare** across all dependent variables. In addition to its potential to destabilise nuclear relations, this application also threatens to cause or intensify harm against civilians. Of particular concern is its potential to further polarise discourses and destabilise trust in information and political processes. Experts noted that it could have particularly negative effects for democracies.

Negative multiplicity also suggests that **these emerging technologies could have more concerning – and as yet unknown – second-order effects on human security**. The capacity to blur the distinction between civilians and the military must be kept in mind by decision makers when further exploring and investing in ASAT capabilities and AI for information warfare.

Experts' concern over the further development and deployment of ASAT capabilities and AI for information warfare can be partially explained by their technological maturity and use. Certain ASAT capabilities, such as kinetic ground-to-orbit capabilities, are comparatively more advanced than other technologies in our study and have already been demonstrated by states. The same can be said about algorithm-assisted information warfare. As discussed in the methods section, we should not discount the potential role of the cognitive heuristics of 'availability' and 'anchoring and adjustment' in influencing our experts' assessments.

These worries might be further heightened when considered in relation to those technologies that are expected to mature more rapidly than others over the next ten years. Our study highlights two ‘rapid destabilisers’, both with a particularly high negative impact score for crisis stability: **hypersonic weapon systems and DEWs are expected to make a significant jump in terms of their deployability by 2030**. It is reasonable to assume that this result reflects – at least in part – the ‘hype’ surrounding hypersonic weapon systems and predictions of an ongoing arms race. In comparison, synthetic biology, ranked most concerning in terms of its expected negative impact on humanitarian principles, is expected to reach deployability at a much slower pace. These results could be important for international regulation efforts. It could help decision makers to focus their attention on those technologies that combine high impact with a rapid pace of deployability in the years ahead.

On the other side of the equation, the expected **positive effects of AI and quantum for C4ISR** purposes are worth mentioning. They include, *inter alia*, improved information, situational awareness, and confidence. These effects, experts concluded, could contribute to mitigating the risk of inadvertent escalation in a crisis.

**Our study underscores the negative environment created by high geopolitical tensions.** The paradigm of great power competition and the apparent prestige that comes with technological innovations were repeatedly cited as being among the main drivers of R&D. Experts highlighted the dominant role of the United States and continued or rising U.S. investments across all technologies. Somewhat inversely, experts pointed to Russian and Chinese efforts to close the competitive gap with the United States by investing in comparably cheaper technologies to offset U.S. dominance (e.g., AI for information warfare). This is another possible instance of Western experts’ bias, wherein the expected ‘catching up’ of U.S. competitors led to negative assessments. In any case, the survey results exhibit a high degree of technology trajectory alignment for the three countries over the next twenty years, for all twelve technologies. These findings point to **a perception among experts that the race for emerging technologies between the United States, Russia, and China is already underway.**

Russia’s status in the context of emerging technologies is somewhat puzzling for experts. The uncertainty surrounding Russia’s general technological trajectory and its ability to compete with the United States was already a matter of

debate among experts in this field before the war in Ukraine. Given the manifold economic, financial, and technological sanctions imposed on Russia after its renewed attack on Ukraine, the existing barriers to Russia's acquisition and deployment of emerging technologies on a broad scale might only increase in the years ahead.

Despite these uncertainties, **the aligning technology development trajectories of China and Russia, when viewed in combination, point to significant deterrence challenges for the United States** and its allies. The expected acquisition of the twelve surveyed technologies by these two U.S. peercompetitors should be viewed in light of the increasingly close strategic relationship – if not outright alliance – of Russia and China. Together, their military-technological capabilities could perhaps even offset some U.S. military advantages by the year 2040.

**Our findings anticipate significant difficulties in the context of arms control.**

The negative environment created by technological and military competition and the alignment of the great powers' technological trajectories suggest that it will be even more difficult to bring these countries on board to regulate emerging technologies in the future. A perception of impending technological parity between the great powers may be sufficient to intensify competition, even if that perception does not line up with reality. Under these conditions, the United States, Russia, and China may be reluctant to negotiate weapons control, preferring unfettered competition in the short to mid term. Unexpected negative knock-on effects are equally possible. Experts cautioned that the proliferation of certain technologies, such as ASAT capabilities, could also negatively affect existing arms control and non-proliferation efforts in other areas, the NPT in particular.

**Then again, arms control may seem more attractive when adversaries narrow the competitive gap.** In other words, if states who once had a monopoly on a technology face the risk of having that technology used against them, they might be more likely to enter arms control talks. In this scenario, the perception that states are more closely aligned in terms of technological capacity and developmental trajectory may be to the benefit of arms control efforts. In the case of hypersonic weapon systems, future bilateral – or even trilateral – formats between the United States, Russia, and China could help address the issue.

**Governing negative multiplicity means recognising the interactive potential of emerging technologies.** This will become particularly important for arms control efforts. Going forward, it may prove difficult to regulate technologies sequentially, based on a pre-specified determination of urgency or achievability. Rather, controls may need to be conceived with multiple innovations in mind, which aim to avoid the effects of specific technologies. A precedent from the past could be the U.S.-Soviet Anti-Ballistic Missile Treaty, which limited the potentially destabilising effects of a specific technology on the strategic relationship of the superpowers. By establishing a linkage between limits to strategic offensive and defensive missiles, negotiators paved the way for addressing this technology.

In any case, **the window for preventive arms control could soon close.** Our experts anticipate that all twelve technologies will reach operational deployability by 2040 in the United States, Russia, and China. This finding should nevertheless be taken with a grain of scepticism, given the artificial end date of our study and experts' uncertainty about Russia's general economic-technological trajectory.

Finally, **narratives matter when discussing the impact of emerging technologies.** Is China's rise inexorable or faltering? Is the United States in decline or resurgent? Have Russian military forces been exhausted or merely set back? The way in which experts approach and answer these questions will influence their perception of the likelihood and intensity of future competition, which may in turn shape their perceptions on matters such as the feasibility of arms control. Among the many difficulties associated with expert foresight – also partially apparent in our study – is the reification of experts' belief systems into reality, however inadvertently. We therefore urge the reader to take this into account. This report clarifies expert *perceptions* surrounding the current and future technological landscape, not objective reality. Given the uncertainty inherent to technological developments, we deem it necessary to also leave open possibilities about 'black swans' and/or the possibility that technologies could evolve at a different pace than our experts predicted.

Beyond any justified scepticism, we hope that our study will contribute to a renewed scholarly debate. Negative multiplicity highlights the limits of examining military innovation in isolation. Instead, scholars should broaden their view and look beyond the immediate effects of emerging technologies. To mitigate the future impact of emerging technologies, scholars and decision makers alike should focus on their potentially negative second-order effects on human security and their possibly destabilising multiple effects during peacetime and in times of crisis.

## Endnotes

- 1 For this study, we use ‘arms control’ as an umbrella term to capture bilateral, multilateral, nuclear as well as non-nuclear limitations and reductions (cf. Larsen 2009). Non-proliferation and risk-reduction measures explicitly fall under this understanding.
- 2 We selected these twelve emerging technologies based on an in-depth review of the existing literature on emerging technologies (Armstrong and Sotala 2015; Bechtel and Buchholz 2022; Drezner 2019; Horowitz 2020; Kunertova 2021; Tracy and Wright 2020), military-technological trends and governance (Affan Ahmed, Mohsin, and Ali 2021; Andås 2020; Ayoub and Payne 2016; Bellasio et al. 2021; Cummings 2017; Gartzke and Lindsay 2019; Kott and Perconti 2018; Krelina 2021; Lieber and Press 2017; NATO 2020; O’Hanlon 2018; Rodriguez 2020), the impact of various technologies on international stability (Boulanin 2019; Chyba 2020; Cox and Williams 2021; Favaro 2021; Johnson 2019, 2021; Kroenig 2021; Nelson 2022; Mazarr et al. 2022; Onderco and Zutt 2021; Saalman 2019; Sechser, Narang, and Talmadge 2019; van Hooft, Boswinkel, and Sweijs 2022; Williams 2019) and human security (Beard 2018; Brundage et al. 2018; Harrison Dinniss and Kleffner 2016; Rejali and Heiniger 2020; Sauer 2021; Shebab 2022; Swanson 2010; Winter 2020).
- 3 Our use of these technology categories was influenced by Kranzberg’s (1986: 547) ‘First Law of Technology’, according to which a technology, such as AI, is ‘neither good nor bad; nor is it neutral’. We took efforts to ensure that all emerging technologies covered in this study were evaluated at the same level of analysis to facilitate their comparison. Some emerging technologies, e.g., quantum technologies, transcend clear-cut categorisations such as military operating domain. By comparing technology applications, we aimed to mitigate this challenge.
- 4 ASAT capabilities are not ‘new’ technologies, but their use against other satellites is concerning for the growing number of state and non-state actors who are reliant upon a sustainable space environment. The development of kinetic anti-satellite capabilities dates back to the early space age (1959), however, the development, testing, and demonstration of such capabilities by the United States, Russia, China, India, and other states is accelerating. Similarly, non-kinetic approaches to denying and degrading satellites via directed energy, electronic interference, or cyberattacks are considered a growing threat.
- 5 We are aware that nuclear instability between other adversaries, particularly in the India-Pakistan context, would also have significant consequences for global security. Our focus on the United States, Russia, and China, however, is due to their comparably greater impact on global security orders, not least due to their increased ability to develop and integrate emerging technologies into their armed forces by 2040.
- 6 According to Ven Bruusgaard and Kerr (2020: 137), ‘the current information environment presents additional challenges for retaining stability in crisis’. This includes new tools of dis- and misinformation and an abundance of unverified data accessible to decision makers.
- 7 When military technologies are created, acquired, or modified, state and non-state actors are obligated to ensure that they comply with the existing rules and standards of war. These rules and standards have legal (i.e., domestic and international law, including international humanitarian law), moral (i.e., ‘Just War Tradition’), and ethical (i.e., military ethics) components. Technologies that are in tension with the humanitarian principles of war may be subject to regulation or, when the tension is intrinsic to the technology, outright prohibition.

- 8 The demographic breakdown of the 30 experts who completed the technology scoring exercise is as follows: 46% of participants were female and 53% male. Of all participants, 23% have been working on topics relevant to this study for 5–10 years, 53% for 10–15 years, and 23% for >15 years. All participants came from Western Europe and North America. The technology forecasting and scoring exercises were sent to experts in September 2021 and returned to us in November 2021. We paid experts an honorarium for their efforts.
- 9 Popper et al. (2007) originally developed STREAM for application in the transportation sector. It has since been applied to a range of security and defence topics (see Bellasio et al. 2021; Favaro 2021). The most recognisable feature of every STREAM application is the technology scoring exercise. In the 1950s and 1960s, researchers at the RAND Corporation advocated for the idea that experts can be used as a source of knowledge about the future (Helmer and Rescher 1960). STREAM builds on this line of thinking. Although the practice of foresight did not originate with RAND, researchers there created a series of techniques aimed at producing knowledge about the future by systematically collecting expert opinions and allowing for a certain degree of interaction among these experts (Dayé 2020). Our study exhibits both aspects of the RAND-prescribed formula.
- 10 Traditionally, STREAM has an equal focus on impact and implementation. In comparison, our study has a greater focus on ascertaining the impact of a given technology and a comparatively lighter focus on the feasibility of that technology's implementation. Our focus on impact can be justified by the fact that STREAM was originally developed to support innovation by a single company in a given sector. Conversely, we use it in this study to gauge the impacts of various technologies on two very broad impact areas: international stability and human security.
- 11 TRL is a commonly used metric for gauging the maturity of emerging technologies (cf. NASA 1976). We adopted the research (i.e., TRL 1–3), development (i.e., TRL 4–6), and deployment (i.e., TRL 7–9) categories as a simplification of the full TRL 1–9 scale from the European Commission (2014).
- 12 When designing the technology scoring exercise, we took care to ensure that the questions were both comprehensive and orthogonal (i.e., statistically independent) so that no value was double-counted.
- 13 The programmer defines the number of clusters. Then, the algorithm partitions the data into the given number of clusters. The algorithm groups similar datapoints into clusters based on a Euclidean distance metric. By partitioning the data into a set of meaningful sub-classes, clustering helps users to understand the structure of a high-dimensionality dataset. In the case of k-means clustering, the algorithm randomly generates the initial 'means'. Clusters are then created by associating every datapoint with the nearest mean. The centroid of each of the clusters becomes the new mean. This is repeated until no centroid changes its value in recalculation, which means that each centroid is the mean of its cluster.
- 14 The Silhouette score is the average ratio between the distances between data points within individual clusters and the distance to the closest data point in separate clusters. In this way, the Silhouette score measures the compactness and separation of each cluster. On the other hand, the Calinski-Harabasz score is the ratio of the sum of inter- and intra-cluster dispersion for all clusters. The higher the Calinski-Harabasz score, the better the performance of a given cluster.

- 15 Our decision not to ask experts for confidence scores is owed in part to the work of Tetlock (2017), who found evidence that experts who are diffident in their predictions are more likely to be right than those who exude confidence.
- 16 There is an ongoing debate on whether experts provide better insights than laypeople. Gordon (1994: 1) assumed that experts' forecasts are more likely to be correct than those from ordinary people. Tetlock (2017) claims that expert judgement about future-related questions is as accurate as random speculations. According to Tetlock, more knowledge does not mean a higher probability of an accurate forecast. Armstrong and Sotala (2015) come to a similar conclusion after assessing 95 timeline predictions in the field of AI. Accordingly, 'expert predictions are greatly inconsistent with each other – and indistinguishable from non-expert performance' (Ibid: 1). Montgomery and Nelson (2020: 9) make the point that experts remain one of the essential sources for forecasts if 'Ideally, the futurists at hand have enough expertise [...] to effectively "connect the dots" where non-experts cannot.'
- 17 To calculate the distance between data points in high-dimensional space, we used the Minkowski Metric with  $r = 1$  (the so-called Manhattan distance, also known as the L1 norm) or  $r = 2$  (also known as the Euclidean distance, or L2 norm). We used the L1 norm, which is preferred for higher-dimensional datasets.
- 18 As explained in the methods section, we used Silhouette and Calinski-Harabasz scores to test the quality of our clusters. Our analysis returned an overall Silhouette score of less than 0.5, which indicates that the average distance between data points in the technology clusters is about half the distance between the cluster centroid and the nearest out-of-cluster data point. This suggests that our research generated reasonably compact and separate clusters, though there is no universal threshold above which a Silhouette score is considered 'good' (Rousseeuw 1987). Given the resulting amount of five clusters, our analysis returned a Calinski-Harabasz score of just over 12. Although there is no 'acceptable' cut-off value (Baarsch and Celebi 2012), graphing Calinski-Harabasz scores for different numbers of clusters showed that five clusters resemble a reasonable fit for our data.
- 19 The term 'negative multiplicity' builds on Rosenberg's (2016: 137) assertion that 'the quantitative multiplicity of societies is also a qualitative one'. According to Wiener (2022: 4–5), 'in qualitative terms, multiplicity implies the recognition of "more than one kind" (i.e. diversity). And, in quantitative terms, multiplicity implies accounting for "more than one" (i.e. plurality).' This perspective is in line with our own findings, where a plurality of different technologies and a diversity of sometimes similar, sometimes different (negative) effects co-exist.



## References

**Acton, James** (2013). Reclaiming Strategic Stability. In: Colby, Elbridge A. & Michael S. Gerson (eds.). *Strategic Stability: Contending Interpretations*. Carlisle Barracks, PA: U.S. Army War College Press: 117–146.

**Acton, James** (2018). Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War. *International Security* 43 (1): 56–99.

**Affan Ahmed, Syed, Mujahid Mohsin & Syed Muhammad Zubair Ali** (2021). Survey and Technological Analysis of Laser and Its Defense Applications. *Defence Technology* 17 (2): 583–592.

**Al-Masri, Anas** (2019). How Does k-Means Clustering in Machine Learning Work? Towards Data Science. <https://towardsdatascience.com/how-does-k-means-clustering-in-machine-learning-work-fdaaf5acfa0> (accessed 24 August 2022).

**Andås, Harald** (2020). Emerging Technology Trends for Defence and Security. Norwegian Defence Research Establishment. <https://publications.ffi.no/nb/item/asset/dspace:6728/20-01050.pdf> (accessed 24 August 2022).

**Armstrong, Stuart & Kaj Sotala** (2015). How We're Predicting AI – or Failing To. In: Romportl, Jan, Eva Zackova & Jozef Kelemen (eds.). *Beyond Artificial Intelligence: Topics in Intelligent Engineering and Informatics*. Cham: Springer: 11–29.

**Asselt, Marjolein van, Susan van 't Klooster, Philip W.F. van Notten & Livia A. Smits** (2010). *Foresight in Action: Developing Policy-Oriented Scenarios*. Oxford: Earthscan.

**Ayoub, Kareem & Kenneth Payne** (2016). Strategy in the Age of Artificial Intelligence. *Journal of Strategic Studies* 39 (5–6): 793–819.

**Baarsch, Jonathan & M. Emre Celebi** (2012). Investigation of Internal Validity Measures for K-Means Clustering. *Lecture Notes in Engineering and Computer Science: Proceedings of the International MultiConference of Engineers and Computer Scientists 2012. IMECS 2012*. 14–16 March. 2012. Hong Kong: 471–476.

**Beard, Jack M.** (2018). The Principle of Proportionality in an Era of High Technology. SSRN. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3119384](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3119384) (accessed 24 August 2022).

**Bechtel, Mike & Scott Buchholz** (2022). Field Notes from the Future: A Look at Three Emerging Technologies over the Horizon. In: Bechtel, Mike & Scott Buchholz (eds.). *Tech Trends 2022*. Deloitte Insights. [https://www2.deloitte.com/content/dam/insights/articles/US164706\\_Tech-trends-2022/DI\\_Tech-trends-2022.pdf](https://www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf) (accessed 24 August 2022).

**Bellasio, Jacopo, Linda Slapakova, Luke Huxtable, James Black, Theodora Ogden & Livia Dawaele** (2021). *Innovative Technologies Shaping the 2040 Battlefield*. Brussels: European Parliamentary Research Service.

**Bonaccorsi, Andrea, Riccardo Apreda & Gualtiero Fantoni** (2020). Expert Biases in Technology Foresight: Why They Are a Problem and How to Mitigate Them. *Technological Forecasting and Social Change* 151: 119855.

**Borrie, John & Vanessa Martin Randin (eds.)** (2005). *Alternative Approaches in Multilateral Decision Making: Disarmament as Humanitarian Action*. Geneva: UNIDIR. <https://www.unidir.org/files/publications/pdfs/alternative-approaches-in-multilateral-decision-making-disarmament-as-humanitarian-action-314.pdf> (accessed 07 September 2022).

**Boulanin, Vincent (ed.)** (2019). *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Volume I. Euro-Atlantic Perspective*. Stockholm: Stockholm International Peace Research Institute. <https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-i-euro-atlantic> (accessed 24 August 2022).

**Brundage, Miles et al.** (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. arXiv. <https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf> (accessed 24 August 2022).

**Bruusgaard, Kristin Ven & Jaclyn A. Kerr** (2020). *Crisis Stability and the Impact of the Information Ecosystem*. In: Lin, Herbert S., Benjamin Loehrke & Harold A. Trinkunas (eds.). *Three Tweets to Midnight: Effects of the Global Information Ecosystem on the Risk of Nuclear Conflict*. Stanford: Hoover Institution Press: 137–158.

**Byman, Daniel** (2013). *Why Drones Work: The Case for Washington's Weapon of Choice*. *Foreign Affairs* (Jul/Aug 2013): 32–43.

**Chyba, Christopher F.** (2020). *New Technologies & Strategic Stability*. *Daedalus* 149 (2): 150–170.

**Cox, Jessica & Heather Williams** (2021). *The Unavoidable Technology: How Artificial Intelligence Can Strengthen Nuclear Stability*. *The Washington Quarterly* 44 (1): 69–85.

**Cozzens, Susan et al.** (2010). *Emerging Technologies: Quantitative Identification and Measurement*. *Technology Analysis & Strategic Management* 22 (3): 361–376.

**Cummings, Mary L.** (2017). *Artificial Intelligence and the Future of Warfare*. Chatham House. <https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings.pdf> (accessed 24 August 2022).

**Dayé, Christian** (2020). *Experts, Social Scientists, and Techniques of Prognosis in Cold War America*. Cham: Palgrave Macmillan.

**Drezner, Daniel W.** (2019). *Technological Change and International Relations*. *International Relations* 33 (2): 286–303.

**European Commission** (2014). *Horizon 2020 – Work Programme 2014–2015, General Annexes, Annex G, Technology readiness levels (TRL)*. [https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014\\_2015/annexes/h2020-wp1415-annex-g-trl\\_en.pdf](https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf) (accessed 24 August 2022).

**European Parliament Research Service** (2021). *Innovative technologies shaping the 2040 battlefield*. [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690038/EPRS\\_STU\(2021\)690038\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690038/EPRS_STU(2021)690038_EN.pdf) (accessed 7 September 2022).

**Favaro, Marina** (2021). *Weapons of Mass Distortion: A New Approach to Emerging Technologies, Risk Reduction, and the Global Nuclear Order*. London: King's College London.

**Frei, Daniel** (1988). *International Humanitarian Law and Arms Control*. *International Review of the Red Cross* 28 (267): 491–504.

**Gartzke, Erik & Jon R. Lindsay (eds.)** (2019). *Cross-Domain Deterrence*. Oxford: Oxford University Press.

**Gordon, Theodore Jay** (1994). *The Delphi Method*. *Futures Research Methodology* 2 (3): 1–30.

**Gray, Colin S.** (1980). *Strategic Stability Reconsidered*. *Daedalus* 109 (4): 135–154.

**Harrison Dinniss, Heather A. & Jann K. Kleffner** (2016). *Soldier 2.0: Military Human Enhancement and International Law*. *International Law Studies* 92 (432): 163–205.

**Helmer, Olaf & Nicholas Rescher** (1960). On the Epistemology of the Inexact Sciences. Santa Monica: The RAND Corporation. <https://www.rand.org/content/dam/rand/pubs/reports/2006/R353.pdf> (accessed 25 August 2022).

**Hoof, Paul van, Lotje Boswinkel & Tim Sweijts** (2022). Shifting Sands of Strategic Stability: Towards a New Arms Control Agenda. The Hague: The Hague Centre for Strategic Studies.

**Horowitz, Michael C.** (2020). Do Emerging Military Technologies Matter for International Politics? *Annual Review of Political Science* 23 (1): 385–400.

**Johnson, James** (2019). The AI-Cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability. *Journal of Cyber Policy* 4 (3): 442–460.

**Johnson, James** (2021). Catalytic Nuclear War in the Age of Artificial Intelligence and Autonomy: Emerging Military Technology and Escalation Risk Between Nuclear-Armed States. *Journal of Strategic Studies*.

**Kania, Elsa** (2017). China's Artificial Intelligence Revolution: A New AI Development Plan Calls for China to Become the World Leader in the Field by 2030. *The Diplomat*. <https://thediplomat.com/2017/07/chinas-artificial-intelligence-revolution/> (accessed 24 August 2022).

**Kaplan, Abraham, A. L. Skogstad & Meyer A. Girshick** (1950). The Prediction of Social and Technological Events. *The Public Opinion Quarterly* 14 (1): 93–110.

**Kavanagh, Camino** (2019). New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses? Working Paper. Washington D.C.: Carnegie Endowment for International Peace. <https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736> (accessed 25 August 2022).

**Kott, Alexander & Philip Perconti** (2018). Long-Term Forecasts of Military Technologies for a 20–30 Year Horizon: An Empirical Assessment of Accuracy. *Technological Forecasting and Social Change* 137: 272–279.

**Kranzberg, Melvin** (1986). Technology and History: "Kranzberg's Laws". *Technology and Culture* 27 (3): 544–560.

**Krelina, Michal** (2021). Quantum Technology for Military Applications. *EPJ Quantum Technology* 8 (24).

**Kroenig, Matthew** (2021). Will Emerging Technology Cause Nuclear War? Bringing Geopolitics Back In. *Strategic Studies Quarterly* 15 (4): 59–73.

**Kunertova, Dominika** (2021). Weaponized and Overhyped: Hypersonic Technology. *CSS Analyses in Security Policy* 285. ETH Zurich. <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse285-EN.pdf> (accessed 7 September 2022).

**Larsen, Jeffrey A.** (2009). An Introduction to Arms Control and Cooperative Security. In: Larsen, Jeffrey A. and James J. Wirtz (eds.). *Arms Control and Cooperative Security*. Boulder: Lynne Rienner Publishers: 1–20.

**Lieber, Keir A. & Daryl G. Press** (2017). The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence. *International Security* 41 (4): 9–49.

**Mazarr, Michael J. et al.** (2022). Disrupting Deterrence: Examining the Effects of Technologies on Strategic Deterrence in the 21st century. Santa Monica, CA: RAND Cooperation.

**Montgomery, Alexander H. & Amy J. Nelson** (2020). The rise of the futurists: The perils of predicting with futurethink. Brookings. [https://www.brookings.edu/wp-content/uploads/2020/11/fp\\_20201130\\_rise\\_of\\_the\\_futurists.pdf](https://www.brookings.edu/wp-content/uploads/2020/11/fp_20201130_rise_of_the_futurists.pdf) (accessed 7 September 2022).

**Morgan, M. Granger** (2014). Use (and Abuse) of Expert Elicitation in Support of Decision Making for Public Policy. *Proceedings of the National Academy of Sciences* 111 (20): 7176–7784.

**Müller, Vincent C. & Nick Bostrom** (2016). Future Progress in Artificial Intelligence: A Survey of Expert Opinion. In: Müller, Vincent C. (ed.). *Fundamental Issues of Artificial Intelligence*. Synthese Library 376. Cham: Springer: 555–572.

**NASA** (1976). *A Forecast of Space Technology 1980–2000*. Washington, D.C.: Scientific and Technical Information Office.

**NATO Science & Technology Organization** (2020). *Science & Technology Trends 2020–2040: Exploring the S&T Edge*. Brussels: NATO S & T Organization.

**Nelson, Amy J.** (2022). Innovation Acceleration, Digitization, and the Crisis of Nonproliferation Systems. *The Nonproliferation Review*: online first.

**O’Hanlon, Michael E.** (2000) *Technological change and the future of warfare*. Washington, D.C.: Brookings Institution Press.

**O’Hanlon, Michael E.** (2018). *Forecasting Change in Military Technology, 2020–2040*. Washington, D.C.: Brookings.

**Onderco, Michal & Madeleine Zutt** (2021). Emerging Technology and Nuclear Security: What Does the Wisdom of the Crowd Tell Us? *Contemporary Security Policy* 42 (3): 286–311.

**Permanent Mission of the People’s Republic of China to the UN** (2020). Statement of H. E. Mr. Geng Shuang, Head of the Chinese Delegation and Deputy Permanent Representative at the General Debate of the First Committee of the 75th Session of the UNGA. [https://www.mfa.gov.cn/ce/ceun/eng/chinaandun/disarmament\\_armscontrol/unga/t1823441.htm](https://www.mfa.gov.cn/ce/ceun/eng/chinaandun/disarmament_armscontrol/unga/t1823441.htm) (accessed 24 August 2022).

**Popper, R., Michael Keenan, Ian Miles, Maurits Butter & Graciela Sainz** (2007). *Global Foresight Outlook GFO 2007: Mapping Foresight in Europe and the Rest of the World*. The EFMN Annual Mapping Report 2007. European Commission, EFMN.

**Rejali, Saman & Yannick Heiniger** (2020). The Role of Digital Technologies in Humanitarian Law, Policy and Action: Charting a Path Forward. *International Review of the Red Cross* 102 (913): 1–22.

**Reuters** (2020). Russia Says It Has Deployed Kinzhal Hypersonic Missile Three Times in Ukraine. Reuters. <https://www.reuters.com/world/europe/russia-says-it-has-deployed-kinzhal-hypersonic-missile-three-times-ukraine-2022-08-21/> (accessed 26 August 2022).

**Rodriguez, Rockie** (2020). Game-Changing Military Technologies: Adoption and Governance. In: Kosal, Margaret E. (ed.). *Disruptive and Game Changing Technologies in Modern Warfare*. Cham: Springer: 13–29.

**Rosenberg, Justin** (2016). International Relations in the Prison of Political Science. *International Relations* 30 (2):127–153.

**Rousseeuw, Peter J.** (1987). Silhouettes: A Graphical Aid to the Interpretation and Validation of Cluster Analysis. *Journal of Computational and Applied Mathematics* 20: 53–65.

**Saalman, Lora (ed.)** (2019). *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Volume II. East-Asian Perspective*. Stockholm: Stockholm International Peace Research Institute. <https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-ii-east-asian> (accessed 24 August 2022).

**Sauer, Frank** (2021). Stepping Back from the Brink: Why Multilateral Regulation of Autonomy in Weapons Systems Is Difficult, Yet Imperative and Feasible. *International Review of the Red Cross* 102 (913): 235–259.

**Scharre, Paul & Ainikki Riikonen** (2020). *Defense Technology Strategy*. Washington, D.C.: Center for a New American Security. <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Defense-Technology-Strategy-2.pdf?mtime=20201116164927&focal=none> (accessed 25 August 2022).

**Schneider, Jacquelyn & Julia Macdonald** (2022). Looking Back to Look Forward: Autonomy, Military Revolutions, and The Importance of Cost. SSRN. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4001007](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4001007) (accessed 25 August 2022).

**Sechser, Todd S., Neil Narang & Caitlin Talmadge** (2019). Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War. *Journal of Strategic Studies* 42 (6): 727–735.

**Shebab, Firas Mohammed** (2022). Using Artificial Intelligence to Enhance Compliance with International Humanitarian Law. *European Journal of Research Development and Sustainability (EJRDS)* 3 (3): 1–8.

**Snyder, Glenn Herald** (1965). The Balance of Power and the Balance of Terror. In: Seabury, Paul (ed.). *Balance of Power*. San Francisco: Chandler: 184–201.

**Steinbach, Michael, Levent Ertöz & Vipin Kumar** (2004). The Challenges of Clustering High Dimensional Data. In: Wille, Luc T. (ed.). *New Directions in Statistical Physics: Econophysics, Bioinformatics, and Pattern Recognition*. Heidelberg: Springer Berlin: 273–309.

**Swanson, Lesley** (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. *Loyola of Los Angeles International and Comparative Law Review* 32 (2): 303–333.

**Tadjbakhsh, Shahrbanou & Anuradha M. Chenoy** (2006). *Human Security: Concepts and Implications*. London: Routledge.

**Tetlock, Philip E.** (2017). *Expert Political Judgment: How Good Is It? How Can We Know?* New Edition. Princeton: Princeton University Press.

**The Editorial Board** (2022). The War in Ukraine Is Getting Complicated, and America Isn't Ready. *The New York Times*. <https://www.nytimes.com/2022/05/19/opinion/america-ukraine-war-support.html> (accessed 7 September 2022).

**The White House** (2021). Remarks by President Biden in Address to a Joint Session of Congress. April 29, 2021. Speeches and Remarks. <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/04/29/remarks-by-president-biden-in-address-to-a-joint-session-of-congress/> (accessed 24 August 2022).

**Toon, Owen B. et al.** (2019). Rapidly expanding nuclear arsenals in Pakistan and India portend regional and global catastrophe. *Science Advances* 5 (10): eaay5478.

**Tracy, Cameron L. & David Wright** (2020). Modelling the Performance of Hypersonic Boost-Glide Missiles. *Science & Global Security* 28 (3): 135–170.

**Tversky, Amos & Daniel Kahneman** (1974). Judgment under Uncertainty: Heuristics and Biases: Biases in Judgments Reveal Some Heuristics of Thinking under Uncertainty. *Science* 185 (4157): 1124–1131.

**UNIDO** (2019). Bracing for the New Industrial Revolution: Elements of a Strategic Response. Discussion Paper. [https://www.unido.org/sites/default/files/files/2020-06/UNIDO\\_4IR\\_Strategy\\_Discussion\\_Paper.pdf](https://www.unido.org/sites/default/files/files/2020-06/UNIDO_4IR_Strategy_Discussion_Paper.pdf) (accessed 24 August 2022).

**United Nations** (2021). Antonio Guterres, Secretary-General of the United Nations, at the Security Council High-Level Open Debate on United Nations Peacekeeping Operations: Technology and Peacekeeping. UN Web TV. <https://media.un.org/en/asset/k1/k1ltu97g1b> (accessed 24 August 2022).

**UNODA** (2019). Opening Statement of the First Committee of the General Assembly at Its 74th Session. <https://www.un.org/disarmament/wp-content/uploads/2019/10/hr-nakamistu-first-committee-speech-10-October-19.pdf> (accessed 24 August 2022).

**U.S. Department of Defense** (2021). Secretary of Defense Austin Remarks at the Global Emerging Technology Summit of The National Security Commission on Artificial Intelligence (As Delivered). <https://www.defense.gov/News/Transcripts/Transcript/Article/2692943/secretary-of-defense-austin-remarks-at-the-global-emerging-technology-summit-of/> (accessed 24 August 2022).

**Vincent, James** (2017). Putin Says the Nation that Leads in AI ‘Will Be the Ruler of the World’: The Russian President Warned that Artificial Intelligence Offers ‘Colossal Opportunities’ as Well as Dangers. *The Verge*. <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world> (accessed 24 August 2022).

**Wiener, Antja** (2022). Societal Multiplicity for International Relations: Engaging Societal Interaction in Building Global Governance from Below. *Cooperation and Conflict*: online first.

**Williams, Heather** (2019). Asymmetric Arms Control and Strategic Stability: Scenarios for Limiting Hypersonic Glide Vehicles. *Journal of Strategic Studies* 42 (6): 789–813.

**Winter, Elliot** (2020). The Compatibility of Autonomous Weapons with the Principle of Distinction in the Law of Armed Conflict. *International and Comparative Law Quarterly* 69 (4): 845–876.

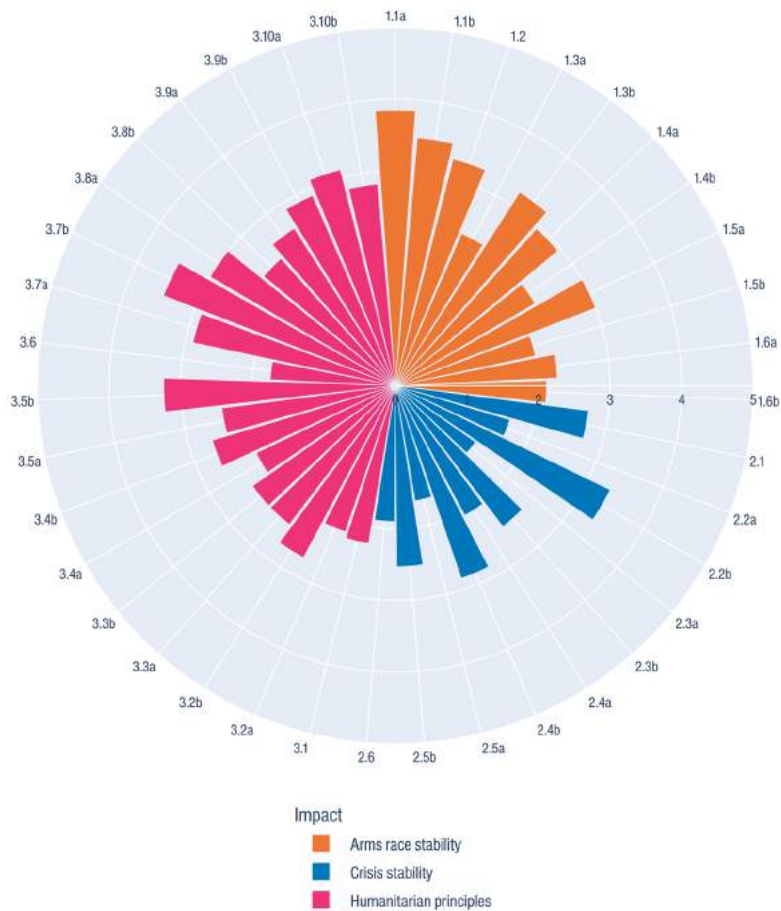
**Wisotzki, Simone & Ulrich Kühn (eds.)** (2021). Crisis in Arms Control. Special Issue. *Zeitschrift für Friedens- und Konfliktforschung*. Wiesbaden: Springer VS.

# Data Annex

This Data Annex contains the mean impact score per question for each technology and an edited collection ('technology deep dives') of experts' qualitative remarks as regards the main barriers to and drivers of the development of these technologies, as well as their respective impact on arms race stability, crisis stability, and humanitarian principles.

## 1 AI FOR C4ISR

**Figure 1: Mean score per question – AI for C4ISR**



## 1.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

The main barriers associated with AI for C4ISR are technical and ethical. According to experts, the United States, Russia, and China share several challenges in developing this technology. This includes difficulties in acquiring representative training data, high error rates, and a shortfall in judgement and abductive reasoning capabilities. Experts also cited legal, ethical, and regulatory barriers, though they anticipated that these would have an uneven impact, with Russia and China being less constrained than the United States.

U.S.-specific barriers include the slow pace of acquisition processes and operational doctrine development, difficulties in integrating this new technology into legacy systems (a challenge the United States shares with China), and a lack of strategic vision regarding the technology. Experts regarded innovation in this area as relatively low cost, suggesting that sufficient funding is unlikely to be an issue for the United States. This is not the case for Russia. In addition to inadequate funding, experts referenced a weaker commercial and technical AI ecosystem in Russia relative to the United States and China. For China, experts cited the government's centralised approach to innovation as a potential barrier. Experts also listed corruption as a challenge for both Russia and China.

According to experts, the military potential of this technology is an important driver for all three states. Possible perceived advantages include faster and more comprehensive analysis of increasingly large and complex data sets, improved decision making, and enhanced signal detection, pattern recognition, and situational awareness. Experts also referenced the potential of AI-enhanced systems to undertake tedious and repetitive human tasks in the context of C4ISR, which could result in enhanced responses to adversary attacks.

AI for C4ISR is an important component of the U.S. strategy for Joint All-Domain Command and Control, which is the U.S. Department of Defense's effort to connect sensors from all military services into a single network. As experts pointed out, however, much of the current enthusiasm for this technology is based on a *perception* of capability that may or may not eventuate. Silicon Valley hype and military-industrial interest group momentum were listed as drivers for the United States. For Russia, experts noted a range of drivers: instrumental factors included a desire to dominate the information environment



and achieve 'reflexive control' in the context of increasingly 'informatised' warfare. Furthermore, experts cited regional security interests, maintaining great power appearances, superpower nostalgia, and technological concerns over falling behind. In addition to a general ambition to compete against the United States, experts noted that China's development of this technology was driven by a desire to optimise its anti-access/area-denial (A2/AD) targeting, better integrate multiple operation domains, and catalyse a shift from 'informatised' to 'intelligentised' warfighting.

## 1.2 IMPACT ON ARMS RACE STABILITY

**This technology, experts argued, will likely provide a range of new offensive options, while also creating new ways to degrade adversary capabilities.**

These anticipated advantages are likely to dissipate, however, as rivals close the competitive gap. The perception that the United States is currently more advanced in its development of this capability – as well as Russia's and China's motivation to address this imbalance – is likely to intensify competition in the years ahead.

**Experts highlighted some potential opportunities presented by AI for C4ISR.**

The acquisition of this technology by U.S. allies could enhance their deterrence options, situational awareness, and attribution capabilities to the potential benefit of regional security. Contrasting this is the risk that adversarial powers will perceive the use of this technology in their region of interest as escalatory and threatening. Experts also made reference to the possibility that accidents and technical malfunctions could worsen regional stability.

**Expert opinion was mixed as to whether this technology would undermine or bolster existing arms control agreements between Russia and the United States.** Experts cited potential improvements to verification and monitoring, though this was counterbalanced by concerns over misinterpretation, deception, and perceived first strike advantages. According to one expert, AI developments in C4ISR may diminish the perceived importance of arms control by giving states more knowledge of the adversary than could be obtained through formal cooperation.

### 1.3 IMPACT ON CRISIS STABILITY

**Experts noted that the impact of this technology on crisis stability depends largely on who possesses it and whether it meets or falls short of expectations.** AI for C4ISR could potentially enhance order formulation, order communication, and strike options, all of which are essential in the early stages of a crisis. The technology could also improve system-wide visibility and analysis as well as interoperability between platforms, services, and allies. This increase in clarity, experts suggested, may mitigate the risk of inadvertent escalation in a crisis.

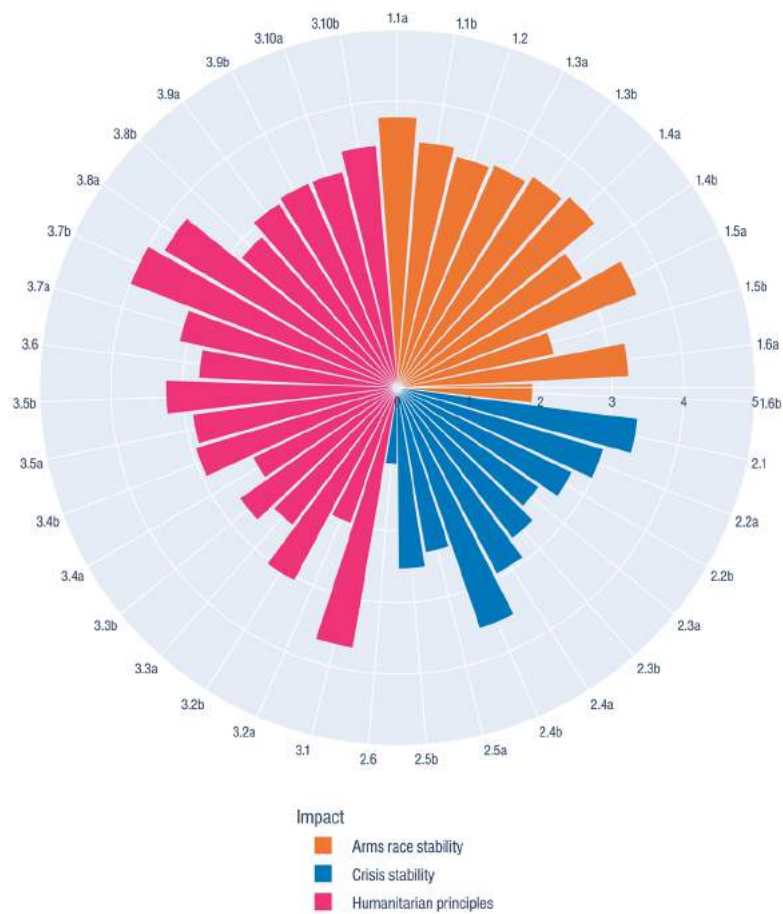
**The identified risks include an overreliance on AI-produced and -sorted information, the potential of adversarial ML and cyber intrusions, as well as errors, biases, and safety/security failures in the system itself.** Experts also referred to the likelihood that innovation in AI will lead to miscalculation, particularly if human operators uncritically accept machine decisions (i.e., automation bias). Compressed windows for decision making could fuel use-or-lose pressures that might destabilise deterrence relationships and intensify crises.

### 1.4 IMPACT ON HUMANITARIAN PRINCIPLES

**Experts offered a mixed assessment of the impact of this technology on humanitarian principles.** AI-enhanced C4ISR may provide some benefits, including improved information gathering and situational awareness, both of which could improve civilian/combatant discrimination. Experts suggested that this technology may also afford decision makers more responsiveness in the formulation of strike plans, helping to mitigate civilian casualties. However, these benefits are heavily dependent on the actual efficacy of the technology: systems without adequate training and testing in appropriate environments, sustained user vigilance and adequate rules of engagement, or systems with biased and flawed algorithms, could jeopardise civilian lives. Experts also expressed concern regarding accountability: AI has the potential to create very real responsibility gaps in the event of unintended harm, while also providing convenient cover for decision maker negligence.

## 2 AI FOR WEAPONS AND EFFECTS

**Figure 2: Mean score per question – AI for weapons and effects**



### 2.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

The main barriers to developing and deploying AI for weapons and effects are technical. Experts highlighted a range of challenges shared by the United States, Russia, and China, including difficulties in acquiring, sorting, and interpreting relevant data, questions surrounding the reliability of ML algorithms, the difficulty of applying this technology in a complex operational environment, and the ongoing susceptibility of this technology to adversary countermeasures.

Several experts argued that AI-incorporated weapons systems are unlikely to meet the technical and military expectations of their advocates.

Experts also identified some state-specific barriers. For the United States, experts cited normative and legal barriers to weapons development and use, as well as a reliance on older legacy platforms. For Russia, they cited a relative lack of wealth and an inferior R&D landscape; for China, they referred to corruption and an authoritarian approach to R&D that could stymie innovation. For both Russia and China, they made reference to a less dynamic private sector.

The two main (and related) drivers of this technology are, first, the anticipated military benefits of AI-incorporated weapons systems and, second, the perception that such technology is necessary to effectively navigate great power competition.

Much of the expert feedback regarding the military potential of this technology related to speed and the perception that such systems will outperform their human counterparts on the battlefield. Experts cited the presumed accuracy and precision of AI inputs as an additional benefit. A final military driver for all three actors was the anticipated ability of this technology to enhance battlefield lethality while mitigating the risk of combatant harm.

Finally, experts cited the competitive geopolitical landscape as a driver: the United States' desire to retain military primacy, China's ambition to establish itself as a peer competitor of the United States, and Russia's desire to maintain its great power status and regional strength.

## 2.2 IMPACT ON ARMS RACE STABILITY

**U.S. spending on military AI is likely to continue and intensify in the years ahead.** Most experts anticipated that the United States will expend significant financial and technical resources to develop military AI with a range of applications, including those that pertain to weapons systems. Experts held mixed opinions on what the acquisition of this technology by non-great powers would mean for arms race stability in East Asia and Europe. One expert described the technology as inherently destabilising, irrespective of specific actors or geographies.

### 2.3 IMPACT ON CRISIS STABILITY

**There is a significant possibility that this technology will weaken crisis stability.** Experts anticipated that AI for weapons and effects – including long-range munitions and drone swarms – could, in combination with other military and non-military measures, support a disarming nuclear first strike, deliver payloads to key NC3 targets, and undertake ‘decapitation’ missions. This was contrasted by those experts who viewed this technology as playing a potentially stabilising role through enhanced deterrence, specifically by providing U.S. allies with a force multiplier that could discourage aggression from significantly larger Russian and/or Chinese conventional forces. This optimism was caveated, however, by a warning of the likely destabilising effect of ‘rogue power’ acquisition.

**Experts cited the technology’s potential capacity to enhance information gathering as a possible benefit in a crisis context** but stressed that this advantage was contingent on the quality of the information received. Inaccurate and corrupted data could worsen decision making processes and exacerbate crisis instability. Uncertainty regarding the reliability of information also influenced expert opinion regarding the potential of this technology to speed up decision making, and whether such an outcome would be a net positive in a crisis.

### 2.4 IMPACT ON HUMANITARIAN PRINCIPLES

**Experts anticipated that the humanitarian impact of this technology will be significant.** This can firstly be seen in relation to the principle of discrimination. Several experts highlighted the problem of incomplete, inadequate, and flawed targeting data, as well as existing AI biases against certain ethnicities and/or gender identities. These limitations would be especially difficult to navigate in complex and dynamic battlefield environments, where delineating between legal and illegal targets is already difficult. Experts cautioned that if the moral and legal challenges associated with this technology are not properly addressed, the vulnerability of the already vulnerable could increase through false target identification and unacceptable levels of collateral damage.

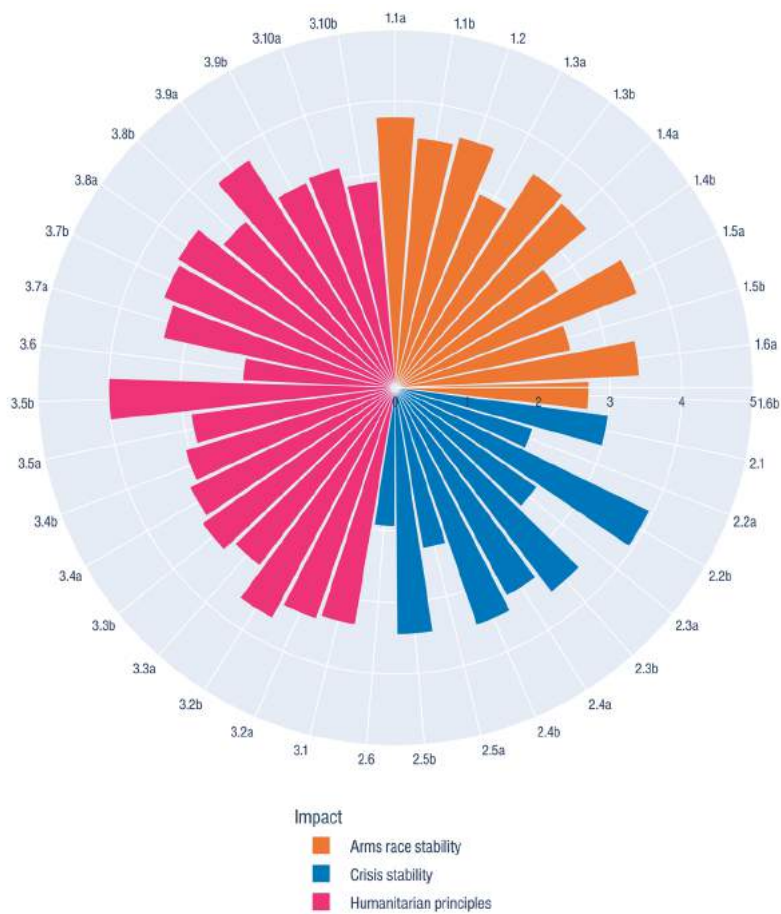
Additional expert concerns related to the erosion of battlefield accountability, a loss of meaningful human control over key military decisions, the inhumanity

of autonomously executed lethal strikes, and the potential for adversaries to exploit system vulnerabilities for tactical and propaganda advantage. Experts also noted this technology's potential capacity to reduce the risk of injury and death for combatants in war. While this has obvious benefits, it may also, experts suggested, lower the political threshold for resorting to war. Lastly, several experts made reference to the possibility of this technology being directed inward, against the domestic populations of those who have access.

**Some experts highlighted the possibility that the adoption of this technology could lead to an increase in civilian protection**, by enhancing battlefield awareness, information gathering, and targeting precision. Overall, however, this optimism was muted, with concerns over whether states (particularly Russia and China) would have the capacity or the desire to bring their innovations fully into alignment with the existing ethical and legal standards of war.

### 3 AI FOR CYBER OPERATIONS

**Figure 3: Mean score per question – AI for cyber operations**



#### 3.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

The main barriers to implementing AI for cyber operations are technical. The ML elements central to AI cyber operations have, to date, been developed in a closed environment and with a narrow focus. Operating this technology effectively in an open environment is significantly more challenging, and experts noted the difficulties associated with designing AI that can detect and intercede incoming cyberattacks.

For the United States, experts listed the following as potential barriers: a relative lack of suitably qualified and experienced personnel; cultural and societal opposition to using AI in this context; and a misalignment between private and public interests in relation to the development of this technology. For Russia, experts listed insufficient funding and R&D limitations as barriers, worsened by an underdeveloped private sector. Private sector challenges also applied to China, according to the experts. Experts further noted that a lack of collaborative partners and an R&D focus heavily tied to the objectives of the People's Liberation Army may hinder innovation in this area.

The main driver of this technology is human limitations in this area: specifically, the inability of humans to monitor entire networks and systems continuously and in real time. Simultaneously, malware and other types of cyberattacks are becoming increasingly sophisticated due to the rapid pace of innovation in ML and AI. According to experts, more advanced AI-assisted cyber operations may be used offensively to detect vulnerabilities and degrade adversary systems, and defensively to safeguard critical national security infrastructure through early detection and automated responses. Experts did note, however, that in practice the distinction between offensive and defensive capacities is often blurred.

Experts anticipated that AI-enhanced cyber operations will play a central role in Russia's security and defence strategy in the years ahead, given what they see as Russia's current operational edge in this domain. China is also expected to heavily invest in this technology, given its already sophisticated hacking operations at present, particularly in corporate contexts. The competitive environment around military AI cyber operations will also, experts anticipated, make this technology a high priority for the United States, with increasing financial and technical investment expected.

### 3.2 IMPACT ON ARMS RACE STABILITY

**Although experts recognised the potential of this technology to enhance regional stability by strengthening deterrence, they considered the inverse a more likely prospect.** AI cyber operations will, experts anticipated, lead to more complex and destructive covert activities and intensify competition in cyberspace. Competition of this type could spur a 'cyber arms race' to the detriment of regional stability and security.



**Experts highlighted the current lack of formal regulation in this area.** The clandestine nature of this technology and resistance from the United States, China, and Russia to meaningful control measures (beyond non-binding normative agreements and confidence building measures) are important factors to consider in this context. Some experts did, however, suggest that this technology could strengthen arms control by improving monitoring and verification.

### 3.3 IMPACT ON CRISIS STABILITY

**This technology poses several challenges to crisis stability.** While AI-cyber operations rarely have a kinetic effect, experts anticipated that when used in concert with kinetic means, this technology could serve as a force multiplier (including in relation to a disarming first strike). The potential for AI-enabled cyber operations to pose new challenges to integrated and connected command and control systems may also worsen crisis stability going forward. Experts further warned of the possibility of accidents due to system fog, faulty understandings of AI-triggered processes, and reduced/ceded human agency. They also highlighted the potential for direct interference by adversaries, for example by corrupting or disabling information gathering in a crisis, which could undermine situational awareness and decision making. These risks may heighten the probability of inadvertent escalation against the backdrop of great power competition.

**If integrated defensively, experts noted this technology's potential capacity to bolster confidence in NC3 systems** by pre-emptively detecting and addressing vulnerabilities and enhancing encryption. Experts noted that if this technology provides new and superior options for acquiring intelligence, then it could strengthen the decision making of those empowered.

### 3.4 IMPACT ON HUMANITARIAN PRINCIPLES

**According to experts, AI cyber operations have the potential to both negatively and positively affect the safety and protection of civilians.** If this technology enables greater operational clarity and predictability through improved information collection, then it may increase belligerents' ability to mitigate civilian harm in combat. Experts also made reference to the possible

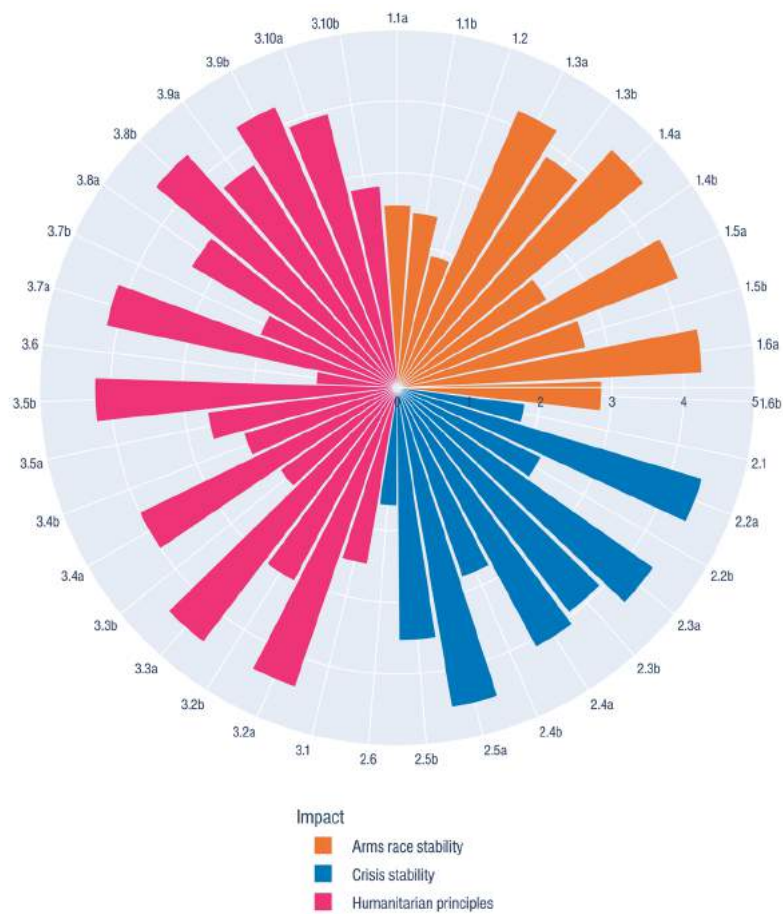
benefits for civilian safety if AI cyber operations are increasingly favoured as a substitute for kinetic action. Contrasting this, however, were concerns that this technology could corrupt or distort critical information, either accidentally or by design, thereby undermining battlefield situational awareness to the detriment of civilian safety.

**Experts also noted the difficulty of discriminating between military and non-military objects in the context of cyber operations.** The interdependency and interconnectedness of networked systems and critical infrastructure (e.g., hospitals, energy grids) suggests that AI cyber operations could indirectly – and perhaps unintentionally – harm civilians. Experts warned that false perceptions of cyberattacks as incapable of causing physical harm and military systems as fully siloed from civilian ones could weaken human oversight and intensify risks to civilians.

**Experts also expressed concerns regarding accountability and attribution.** AI cyber operations are likely to be utilised by security services and non-state actors in a covert and deniable manner. Attribution challenges, experts argued, will likely intensify if AI can enhance the ability of actors to effectively spoof adversarial capabilities. This could negatively impact human security, enabling actors to escape accountability for criminal attacks. However, some experts did recognise AI's potential to enhance attribution via advanced digital forensics.

## 4 AI FOR INFORMATION WARFARE

**Figure 4: Mean score per question – AI for information warfare**



### 4.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

According to experts, the main barrier to deploying this technology for the United States is political and public unease concerning social engineering and psychological operations, as well as the criticism likely to follow in the wake of its use. However, experts also noted that, given the high level of secrecy surrounding this technology, it is difficult to predict the extent to which public unease would pose a hindrance. The main barrier to applying this technology in

a military context for Russia is the anticipated ability of its private sector to scale its use. Moreover, the technical barriers to developing this technology are low, making it an attractive option for state and non-state actors alike.

According to experts, Russia is particularly interested in developing this technology. This is in part because using AI to enhance active measures and influence campaigns seemed to experts to be a natural outgrowth of Russia's history of information operations. Second, this technology does not involve highly expensive platforms, meaning that Russia can compete with the United States and China. Third, information operations are a key part of sub-threshold warfare and gaining the advantage in the initial stages of war, which is, according to experts, central to Russian military doctrine. Meanwhile, experts anticipated that the United States will primarily invest in counter-influence AI measures to combat the risk that information operations pose.

On the domestic level, experts noted that given Chinese restrictions on internet usage, this technology could supplement efforts to maintain domestic stability through the control of information. On the international level, experts raised the possibility that China could follow the Russian example of using information operations against American constituencies, though they cautioned that, to date, China has seemed more interested in using information operations in a regional context against Taiwan and Hong Kong.

## 4.2 IMPACT ON ARMS RACE STABILITY

**Distrust is not conducive to negotiating and/or upholding arms control agreements.** Experts noted that the aim of this technology is to destabilise and subvert relationships. They underscored the potential for distrust and contaminated information environments to erode institutions and uproot deeply held societal norms.

**Mis/disinformation could complicate verification and monitoring,** which, experts noted, could lead to incorrect conclusions about intentions and capabilities. According to experts, this effect may not be equally distributed, since not all states would be equally impacted by disinformation: wealthier states have more robust national technical means to analyse text, images, video, and audio for signs of manipulation. Even if verification and monitoring data is not

manipulated, the perception that it *could* be manipulated may be sufficient to lower confidence levels.

#### 4.3 IMPACT ON CRISIS STABILITY

**Experts were reluctant to draw a direct causal connection between this technology and the threat of a disarming first strike.** While synthetic media could theoretically result in the use of nuclear weapons (e.g., a deep fake video of a head of state ordering their use), several verification measures would need to fail for such an order to be followed. Experts noted that it is more likely that this technology would complement a kinetic strike or cyberattack. In these cases, the objective could be to throw the target off-guard before a strike and/or delay a response until it is too late.

**Decision makers are more susceptible to influence than NC3 is susceptible to intrusion.** Experts noted that, while intrusion into NC3 is – in principle – difficult, influencing individuals in or close to the chain of command is less challenging. This technology could muddy the strategic waters for decision makers, even if they give more credence to intelligence reports and internal briefings than they do to live news and social media feeds. Experts feared that the compound effect of sustained information operations could create divides amongst national security staffers with regard to threat perception, including what information they find credible. Finally, this technology could destabilise public opinion and put pressure on decision makers to act quickly in a crisis.

#### 4.4 IMPACT ON HUMANITARIAN PRINCIPLES

**This technology may blur the distinction between civilians and combatants** in two ways, according to experts. First, information warfare is often designed to indiscriminately sow discord, distrust, and doubt within a target population. This is especially true when synthetic media is transmitted over social media platforms. Second, synthetic media is often created, disseminated, and amplified by civilians who may or may not have ties to the state but cannot be legally targeted with lethal force.

**Targeted and tailored information could modify individuals' cognitive and/or emotional abilities.** Synthetic media is a useful tool for emotional manipulation because it affects our ability to believe what we see with our own eyes. It seemed plausible to experts that information operations targeting decision makers before a crisis could alter their cognitive abilities during that crisis. This technology could desensitise the public to harm, injury, and damage. Experts also considered the effect of propagandistic imagery of violent deaths, disasters, and/or atrocities. They suggested that this could lower a population's moral resistance to inhumane acts by dehumanising and/or mischaracterising the enemy.

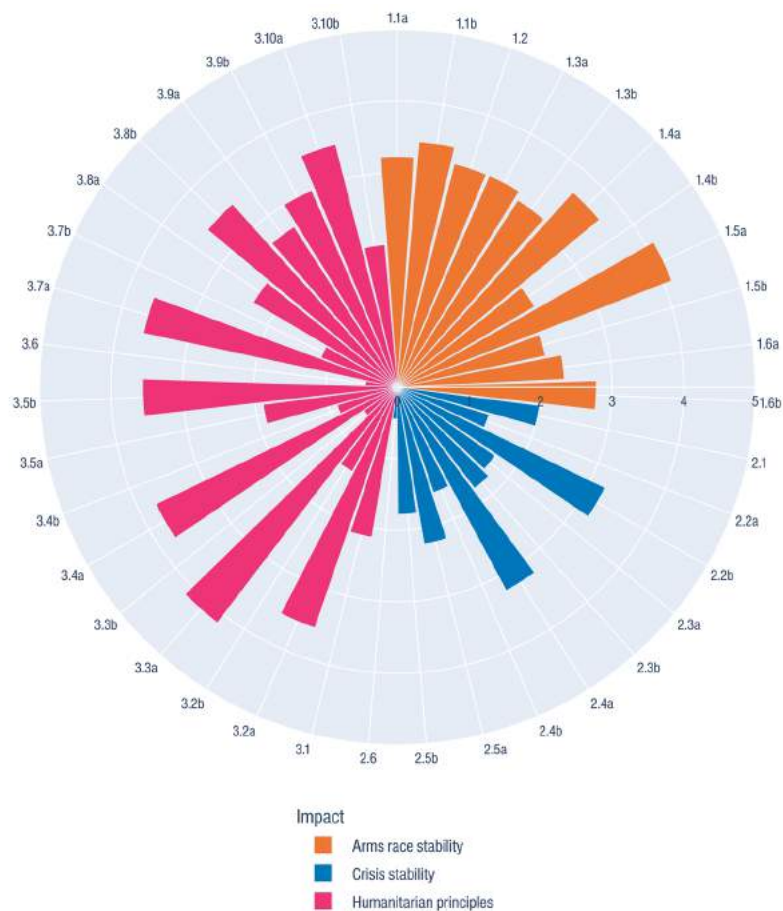
**By exploiting existing social biases and stereotypes in civilian groups, this technology could increase the vulnerability of protected persons.** Experts noted that the use of existing social biases to mobilise and radicalise populations has a long history and could be exacerbated by social media and the lack of representation in AI training datasets.

It will be imperative to define and quantify accountability and attribution, particularly insofar as these challenges are intensifying as the technology advances. Given the current difficulty of holding perpetrators to account for mis/disinformation, experts wondered whether liability for AI-enhanced information warfare lies with programmers, bots, hackers, or somewhere else entirely. Complicating the picture further, misinformation spreads rapidly via social media and is difficult to track.

**This technology could stoke polarised sentiments and destabilise trust in political processes.** According to experts, this could increase the likelihood of resorting to the use of force. Furthermore, experts noted that this technology comes with the additional risk of inciting an armed conflict or escalating a crisis.

## 5 QUANTUM FOR HARDENING AND EXPLOITING SYSTEMS

**Figure 5: Mean score per question – Quantum for hardening and exploiting systems**



### 5.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

The main barrier associated with quantum for hardening and exploiting systems is technological. According to experts, the technical barriers to developing this technology include high energy consumption, error rates, ‘noise’ in quantum computers, finding suitably qualified and experienced personnel, sourcing advanced materials with novel quantum properties and technologies,

the development of the necessary software and hardware, integration with or replacement of existing IT infrastructure, and quantum repeaters for quantum key distribution.

Experts noted that China currently stands at the forefront in terms of quantum R&D but continues to face challenges associated with technological readiness. Experts also cited promising developments by private technology companies in the United States but believe that technological breakthroughs remain a distant prospect. Finally, experts mentioned Russia's slow start in this field, static innovation system, relative lack of economic resources, and lack of access to international collaboration as additional barriers.

Experts noted that for the United States, China, and Russia there is a confluence between military, government, and private sector interest in developing this technology. All three states recognise the potential threat to data security and communication channels posed by quantum cryptography and quantum computing. They further recognise a need for secure communication systems and robust encryption technology and acknowledge that this technology could provide secure communications with autonomous systems, decrypt stored intercepted communications (i.e., 'hack now, crack later'), and offer assurances against adversarial decryption capabilities.

Experts noted that China is motivated by a desire to gain technological supremacy, erode U.S. advantages in decryption, and possibly leapfrog conventional U.S. capabilities. Several experts cited competition with China as a significant driver for the United States.

## 5.2 IMPACT ON ARMS RACE STABILITY

**This technology could positively or negatively impact regional stability in Europe and/or East Asia.** Experts noted that if U.S. allies – such as South Korea, Japan, and/or NATO member states – use quantum technologies to improve their cyber defences, this could augment the stabilising effects that those alliances bring to their respective regions. On the other hand, proliferation of this technology could negatively impact regional security if it creates another avenue for arms racing.



**This technology could generate proliferation incentives that could trigger an arms race and pose challenges for multilateral institutions.** Specifically, experts cautioned that the ‘hack now, crack later’ strategy applied to weapons designs could aid vertical or horizontal proliferation. Alternatively, if non-nuclear weapon states’ records of nuclear hedging or non-compliance with the NPT were brought to light, this could create political challenges for the institution.

**This technology could erode or enhance verification and monitoring.** More optimistic experts noted quantum computing’s ability to break encryption, which could improve national technical means by adding a layer of information certainty, reliability, and security. Less optimistic experts noted that quantum hardening could allow some parties to make their activities highly inaccessible to verification and monitoring efforts. The latter group of experts noted that quantum-hardened national technical means – especially if asymmetric – could decrease reliance on, and trust in, measures of control.

### 5.3 IMPACT ON CRISIS STABILITY

**The impact of this technology depends on the balance between offensive and defensive applications.** This technology has the capacity to improve information availability and recall due to faster computing speeds. If such an advantage is gained, however, countermeasures such as relatively quantum-safe cryptosystems (e.g., algorithms, cryptographic hashes, key-derivation functions, and symmetric ciphers) have the potential to neutralise any advantage gained. Experts noted that states could also adjust their nuclear force posture to counter quantum advantage, with potentially destabilising ancillary effects.

**Hardened systems could sever critical intelligence sources.** On the one hand, experts noted that more secure communications could improve situational awareness and stability. On the other hand, they suggested that if cyberespionage becomes more difficult due to quantum encryption technologies, this could undermine the intelligence machinery, which could be destabilising.

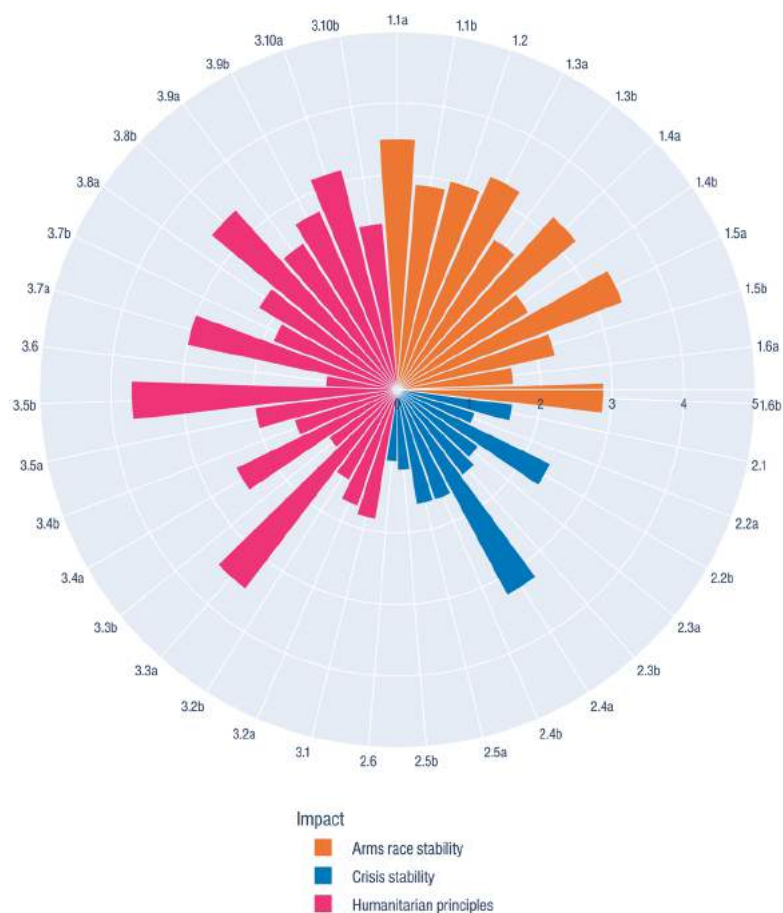
## 5.4 IMPACT ON HUMANITARIAN PRINCIPLES

**This application could exacerbate existing cybersecurity threats to civilians.** If states develop quantum decryption before civilian systems are sufficiently prepared to resist – a likely scenario, according to the experts – then cyberattacks on civilian targets could intensify. The non-consensual harvesting and utilisation of civilian data would have serious ramifications for data privacy and personal integrity, especially for protected persons.

This technology has the potential to increase or decrease attribution challenges. On the one hand, this technology would allow for easier identification of digital vulnerabilities and provide patching solutions. On the other hand, experts noted that this technology could raise certain barriers to attributing attacks. There are, however, likely to be fewer actors with quantum capabilities, at least initially, which would mitigate attribution challenges.

## 6 QUANTUM FOR C4ISR

**Figure 6: Mean score per question – Quantum for C4ISR**



### 6.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

The main barrier associated with quantum for C4ISR is technological; the hardware that accommodates and interfaces with these applications is comparatively immature. According to experts, the technical barriers to developing the hardware include miniaturisation, energy consumption, mobility, connectivity, and challenges associated with surpassing present qubit processing capabilities. Once the technology is sufficiently mature, developers will face

the challenge of scaling it such that it does not create new vulnerabilities when deployed. Several experts emphasised that interfacing with existing systems constitutes the most significant barrier to deploying this technology for all interested states.

Experts noted that this technology could confer meaningful commercial, political, and military benefits. Experts cited five examples; first, quantum key distribution hosted on satellites would represent a significant advancement for C4ISR capabilities. Second, quantum sensors could provide an alternative system for positioning, navigation, and timing, which would enable counterforce options in a GPS-degraded environment. Third, quantum imaging could render nuclear weapon-capable submarines vulnerable to detection – especially in the Arctic – which would degrade the second-strike capability of those targeted. Fourth, given the emphasis that NATO and the United States place on multi-domain operations, this technology could improve real-time information sharing and information security across C4ISR platforms. Fifth, quantum computing could enhance the application of ML to early warning or strike planning, which would improve the speed and effectiveness of these programmes.

This has translated into intense competition between a range of state and non-state actors. According to experts, states are primarily motivated by their interest in systems resiliency. China, the United States, and (to a lesser extent) Russia are also racing to achieve technological supremacy. Experts suspected that China's self-perception as a pioneer in this technology is driving its R&D efforts, which, in turn, has motivated the United States to catch up. For Russia, experts suggested that control of the information environment is a key driver.

## 6.2 IMPACT ON ARMS RACE STABILITY

**Experts anticipated that U.S. military funding for quantum research will increase**, reflecting an acknowledgment that quantum technologies are necessary for securing future C4ISR systems. They noted that if an adversary improves counter-stealth or anti-submarine capabilities through quantum sensing, this could significantly alter strategic capability acquisitions.

**The impact of this technology on existing arms control agreements would depend on relative TRLs.** Experts noted that better C4ISR could increase confidence in arms control reductions. For example, quantum sensing technology could enhance verification by detecting the presence or absence of nuclear material from a greater distance. Experts also cautioned, however, that possible arms control advantages would be unlikely to transpire in negotiations comprised of ‘haves’ and ‘have-nots’. For example, given that Russia is less likely than the United States to develop this technology, they may feel less inclined to participate in future arms control agreements. Mistrust could arise from the knowledge that this technology could be used by its possessors to bypass traditional measures of control. Since the development of this technology is likely to be asymmetric, experts agreed it could harden existing global hierarchies and exacerbate competition.

**Quantum computers could create nuclear proliferation risks.** One expert suggested that if states use quantum computing for nuclear design validation and non-explosive testing, this could make it easier for proliferators to acquire nuclear weapons or improve their designs without risking detection by the Comprehensive Nuclear-Test-Ban Treaty Organization.

### 6.3 IMPACT ON CRISIS STABILITY

**Experts agreed that this technology would improve the overall information landscape** – even in denied/degraded environments – because it would make more information available, process information quicker, and increase confidence in that information. This would enhance transparency and situational awareness, with the caveat that this would result from an extended monitoring period, not a single action. One expert cautioned that increased transparency could beget increased distrust and incentives to better hide military assets.

**Asymmetric quantum capabilities could destabilise a crisis.** If quantum technologies enable states to disrupt – or threaten to disrupt – adversary NC3 during a crisis, this could incentivise an adversary to use nuclear weapons first. Experts emphasised that even a perceived quantum advantage could have a destabilising effect on crisis conditions.

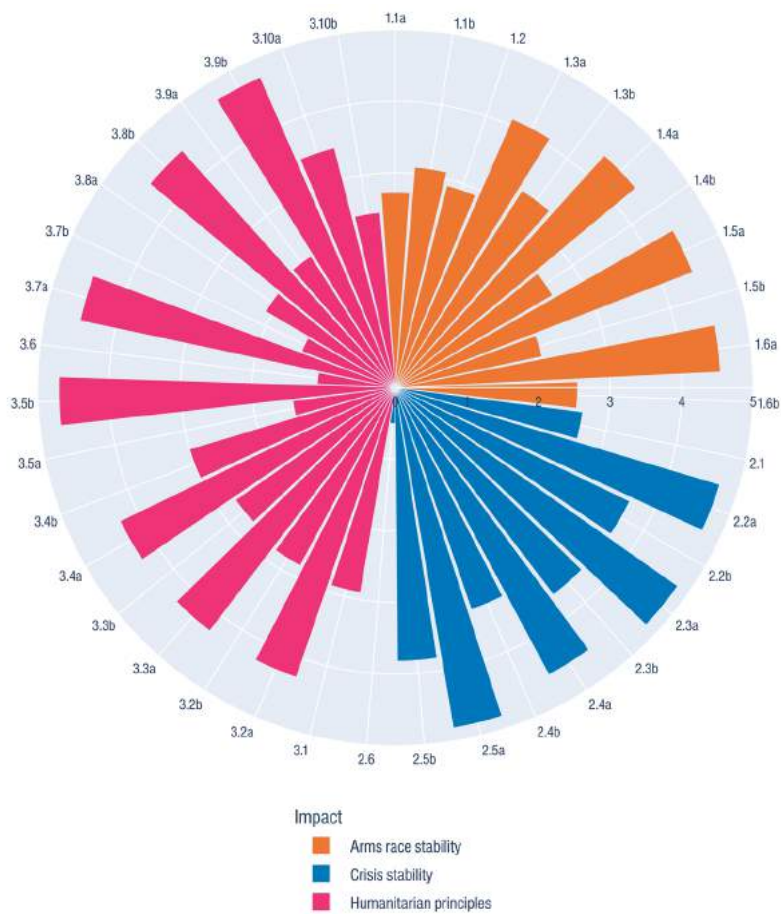
## 6.4 IMPACT ON HUMANITARIAN PRINCIPLES

**This technology could provide new or strengthened tools to promote compliance with the principle of distinction and enhance meaningful human control.** Using quantum communications and sensing in C4ISR could improve the quality of information available, the resiliency of communications, the efficiency of ML models, and overall confidence in NC3. Experts argued that doing so could provide decision makers with more time and options to mitigate unintended harm when using force. Experts agreed that the technology could be helpful in providing more accurate and timely updates of the situation during an attack, which could improve targeting, especially when paired with AI capabilities. A longer decision making window could also strengthen the ability of actors to exert meaningful human control over targeting decisions.

**This technology could give rise to accountability and attribution challenges.** Experts noted that quantum capabilities, when integrated into NC3, have the potential to increase anonymity. This technology could be used to obfuscate the chain of decision making and implementation. This could make it difficult to identify and hold accountable those who violate legal or moral rules in war.

## 7 ANTI-SATELLITE CAPABILITIES

**Figure 7: Mean score per question – Anti-satellite capabilities**



### 7.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

The main barriers to deploying ASAT capabilities in a military context for the United States, China, and Russia are political, rather than technical. Experts cited the lack of institutional support for procuring so-called ‘space weapons’ within the U.S. military and among American audiences as a major barrier. They believe that ASAT procurement is at odds with the United States’ desire to be perceived as a responsible space actor. Similarly, experts noted that Chinese

and Russian proponents of the proposed treaty on the Prevention of an Arms Race in Space are unlikely to support ASAT capability development.

Depending on the type of ASAT capability, there are also barriers related to the sustainability of the space environment. Concerns over unintended consequences of ground-to-orbit ASAT capabilities are particularly acute, given their ability to generate space debris and potentially trigger cascading collisions. The resulting Kessler syndrome would threaten satellite communications and critical infrastructure, with profound and indiscriminate effects on orbit and on Earth.

As satellites and ASAT capabilities proliferate, the United States, Russia, and China perceive a need to deter or defeat hostile activities in space (e.g., ‘blinding’ an adversary and/or undermining communications, targeting, and guidance during peacetime and wartime), which could arise from a growing number of states and commercial actors. Experts also noted the symbolic value of ASATs: testing/demonstrating ASAT capabilities signals a readiness for space warfare. Given their uncertain impact on escalation and deterrence, experts largely deemed it irresponsible for ASATs to target NC3 or military satellite communications.

Experts indicated that the United States is primarily motivated by ambitions of space supremacy; however, they noted that this capability would prove more advantageous to China and Russia, since it could offset other U.S. military advantages. Experts agreed that the United States has more to lose from ASAT use, given its heavy reliance on space for military operations and critical national infrastructure. Disrupting the United States’ access to space and space-enabled data and services has the potential to create significant military gains for China or Russia.

## 7.2 IMPACT ON ARMS RACE STABILITY

**Most experts indicated that ASAT proliferation would be detrimental to terrestrial security.** The United States, Russia, China, and India have developed and tested ground-to-orbit prototypes. Other states that might consider this pursuit include South and North Korea, as well as states who seek to position themselves as space-faring nations, such as France and the United Kingdom.



Experts suggested that capability development by nuclear possessors could weaken international trust and deepen the divide between nuclear weapon states and non-nuclear weapon states, with adverse impacts on multilateral agreements like the NPT. Furthermore, the political posturing associated with ASAT capabilities puts pressure on existing arms control agreements such as New START and contributes to a sense that nuclear risks are growing. The Outer Space Treaty of 1967 does not prevent the use of ASATs as they are currently used (i.e., for posturing), but their use against other states that would represent a challenge to the Treaty's Liability Convention.

**Mutual vulnerability could create the conditions for arms control.** To the extent that proliferation could drive actors to recognise mutual vulnerability, some experts suggested that mutual vulnerability could incentivise the creation of new legal and/or normative arms control mechanisms (e.g., to prevent inadvertent escalation). Recognising the impact that ASATs could have on national technical means of verification could also bring parties to the negotiating table.

According to experts, **states will direct future military spending to enhancing the resiliency and redundancy of space assets to mitigate the impact of ASATs.** Non-materiel solutions such as personnel training could also be helpful to manage the disruption or denial of space-enabled data and services.

### 7.3 IMPACT ON CRISIS STABILITY

**Denying or disrupting ISR, NC3 satellites, and/or orbital early warning systems could be part of a broader campaign to blind an enemy to an inbound attack.** Experts noted that this could trigger conventional and/or nuclear strikes. The extent to which such a strike would qualify as a 'disarming' first strike was considered unclear since no nuclear weapon state is entirely reliant on space-based nodes for their nuclear forces. Experts noted that responding with nuclear weapons would still be possible. Although experts anticipated that the use of ASATs will degrade situational awareness and put pressure on decision makers to act quickly, they also noted that situational awareness is not produced exclusively by space-based capabilities.

**Experts highlighted a perceived first-mover advantage associated with this technology**, wherein states believe that striking an adversary's space-based assets could provide them with a military advantage if done first. Different types of ASAT capabilities come with different attribution challenges, however: whereas ground-to-orbit ASATs can be attributed via space situational awareness capabilities, co-orbital and non-kinetic (i.e., cyber, electronic warfare) ASATs are more likely to create attribution challenges.

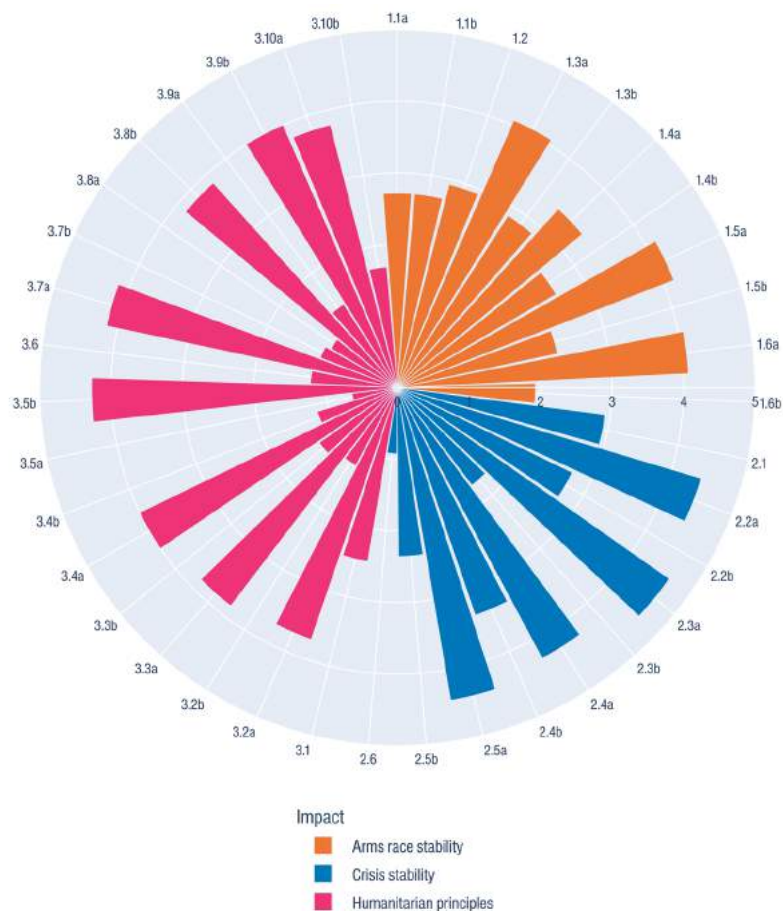
#### 7.4 IMPACT ON HUMANITARIAN PRINCIPLES

**This technology could have damaging second-order effects on populations.** The second-order effects of ASAT use (e.g., disruption to critical national infrastructure, the economy, and the internet) could be profound and indiscriminate, especially considering the growing societal dependency on space-enabled technologies like IoT devices and self-driving cars. According to experts, this damage could eventuate for two key reasons. First, many satellites are dual use (i.e., civilian and military). Second, space debris poses a risk to all satellites within an affected orbit, especially in the event of a collisional cascade. Experts further cited the possibility that the use of ASATs during a conflict could spur escalation on Earth, potentially including the use of nuclear weapons.

**In a crisis, the potential loss of military satellite communications with or between fielded forces could affect control over a variety of operations.** It could, for example, interfere with remotely controlled uncrewed systems, forcing operators to revert to line-of-sight datalinks or autonomous mode. Experts noted that this would likely weaken the ability of actors to exert meaningful human control over targeting decisions.

## 8 HYPERSONIC WEAPON SYSTEMS

**Figure 8: Mean score per question – Hypersonic weapon systems**



### 8.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

Experts cited three relevant features of hypersonic weapon systems: speed, stealth, and manoeuvrability. First, speed is supposedly what sets hypersonics apart. However, experts disputed whether they will be faster than ballistic missiles, even in the best of circumstances. Experts noted that hypersonics cannot match the short delivery times of depressed submarine-launched ballistic missiles, though they exhibit a modest advantage over ballistic missiles

flying minimum energy trajectories. The second feature is stealth. Proponents argue that hypersonic vehicles travel so fast they ionise the air around them, forming a plasma that makes the vehicle invisible to radar, leading experts to suggest that this would increase the ‘fog of war’. However, some experts doubted that hypersonic glide vehicles can manage their speed in a way that tailors the plasma envelope. This makes them unlikely to have a radar signature that is meaningfully smaller than those of comparable ballistic missiles. Third, some experts noted that a manoeuvrable payload could be useful for striking mobile strategic targets, evading ballistic missile defences, and increasing the likelihood of a disarming first strike. However, other experts cautioned that manoeuvrability will likely only make hypersonic vehicles marginally more effective, since turning at hypersonic speeds could knock them off course and decrease their accuracy.

Certain features of hypersonic weapon systems pose enduring technical barriers for the United States, China, and Russia. This includes materials science advancements for dealing with the heat generated during flight, improved scramjet propulsion technology, and better communication with the re-entry vehicle. Non-technical concerns raised by experts include the lack of a clear mission, uncertainty regarding performance, bureaucratic limitations, the enormous cost of such systems, and their uncertain impact on deterrence.

Experts agreed that the most significant driver of this technology is great power competition. According to experts, the United States, China, and Russia are currently engaged in an arms race motivated by the exclusivity of this capability, the political prestige it confers, and a perceived first-mover advantage. The United States is specifically motivated by the potential benefits of long-range hypersonic weapons vis-à-vis China, given the vast distances involved in any conflict in the Indo-Pacific. For Russia and China, the ability to circumvent ballistic missile defences and gain a possible conventional advantage over the United States is considered a primary driver of this capability. Finally, experts asserted that hypersonics will be central to maintaining China’s regional hegemony: due to their ability to target adversary ships and bases in the region, these systems could be used to penetrate A2/AD installations.

## 8.2 IMPACT ON ARMS RACE STABILITY

**Hypersonic weapon systems development enjoys significant political support in the United States.** Political support in the United States is substantial, suggesting that hypersonics could represent a significant portion of future U.S. military spending, according to experts. The development of hypersonic systems by U.S. adversaries may also drive investment in counter-hypersonic systems such as directed energy weapons.

**Mutual vulnerability could create the conditions for arms control.** Some experts suggested that proliferation could force adversaries to acknowledge their mutual vulnerability, which might bring parties to the negotiating table. Other experts tempered this optimism by noting that the ongoing hypersonic arms race is fuelling distrust between states, reducing states' willingness to participate in arms control, and complicating the negotiation of future treaties.

**This technology could act as a driver of the TPNW.** According to experts, the fact that nuclear weapon states have developed this technology for nuclear missions (e.g., Russia's 'Avangard' system) could lower the confidence of non-nuclear weapon states parties to the NPT. Non-nuclear weapon states may regard hypersonics with nuclear payloads as defying the spirit of the NPT's Article VI disarmament obligations. Since confidence in the NPT is an essential foundation for the pursuit of nuclear weapons, experts suggested that this could prompt non-nuclear weapon states to look to alternative governance mechanisms, such as the TPNW.

According to experts, **hypersonics are likely to make verification and monitoring more challenging**, given that they are hosted on various platforms and can be fitted with both nuclear and conventional warheads.

## 8.3 IMPACT ON CRISIS STABILITY

**Hypersonic weapon systems will impact crisis stability in three ways**, according to experts. First, due to their high precision and relatively long range, hypersonics constitute an ideal weapon system for destroying, damaging, or degrading NC3 deep inside enemy territory. This could undermine the target's ability to retaliate. Second, targeting and warhead ambiguity could intensify

instability and incentivise crisis escalation. Third, the ‘use it or lose it’ dynamic created by short warning times could lower the threshold for initiating war and create an advantage for the first mover. At the same time, experts noted the lack of a clearly defined military requirement for this capability and questioned the strategic utility of hypersonic cruise missiles and hypersonic glide vehicles over existing ballistic and cruise missiles.

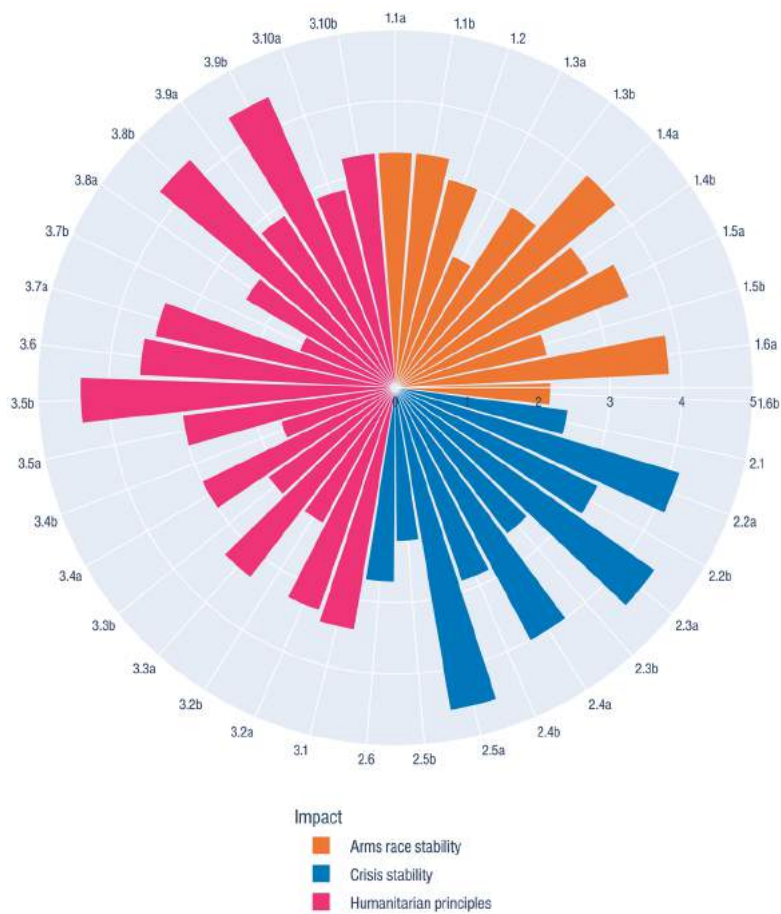
#### 8.4 IMPACT ON HUMANITARIAN PRINCIPLES

**Hypersonics could reduce collateral damage.** Experts noted that the accuracy and manoeuvrability of conventionally armed hypersonic weapon systems could enhance the precision of attacks, enabling belligerents to limit or avoid civilian casualties. To the extent that a hypersonic weapon system constitutes a conventional alternative to a nuclear strike option, it could also allow for more proportionate uses of force.

**Hypersonics could reduce meaningful human control in attacks.** Experts noted that the anticipation of compressed decision making time could push leaders to rely on automated or semi-automated command and control of these systems. If the targeting and/or guidance of the weapon is delegated to automated or autonomous systems, human oversight and control could be reduced in such a way as to undermine compliance with the laws of war.

## 9 DIRECTED ENERGY WEAPONS

**Figure 9: Mean score per question – Directed energy weapons**



### 9.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

For the United States, Russia and China, experts agreed that the main barriers to developing and deploying DEWs in a military context are size, weight, and power requirements, especially related to their integration into smaller platforms. Experts also cited the need for dedicated and highly skilled operators and personnel, technical barriers including energy storage, relevant ethical and legal considerations, and the overarching cost and complexity of this technology.

One expert noted that Russia must contend with the impact of sanctions on domestic defence and electronics industries, while other experts mentioned that Russia is suspected of having used microwave radiation against U.S. officials.

There are several applications for DEWs, but the most prominent are missile defence and anti-satellite capabilities. Experts noted that the tactical benefits of DEWs include rate of fire, speed of travel, scalability of effect, magazine depth (i.e., the ability to produce a potentially unlimited and unconstrained number of shots), and improvements to targeting. This culminates, according to experts, in a controllable and bespoke defensive or offensive capability.

Experts highlighted the defensive potential of DEWs for countering rocket, artillery, and mortar; countering unmanned aerial systems; offsetting adversary forces/swarms; and defending against hypersonic weapon systems. Regarding the offensive capabilities of DEWs, experts noted that lasers or high-power microwaves could damage or disable electronics without causing harm to humans. However, DEWs may also be used in an anti-personnel manner.

## 9.2 IMPACT ON ARMS RACE STABILITY

**Experts primarily view DEWs as a defensive capability for the United States.** The United States has been funding DEWs via their ballistic missile defence (BMD) research programmes for decades. Experts anticipate that this will continue and that the military budget allocated to DEWs might increase considering the perceived threat that hypersonic weapon systems pose to traditional missile defences.

**DEWs could undermine mutual vulnerability and/or incite an arms race.** Some experts suggested that this technology would increase the cost of a Chinese or Russian campaign, thereby strengthening deterrence, encouraging restraint, and contributing to international stability. However, other experts noted that China and Russia could view the use of DEWs for BMD as undermining mutual vulnerability. This could result in increased Chinese and Russian military spending on offensive capabilities that can overcome U.S. missile defences. One expert noted that if China and Russia augment their missile defences with DEWs, this could incentivise countries in their respective neighbourhoods to offset this asymmetry. In this instance, the presence of these weapons would create regional instability, resulting in a 'zero-sum' arms race.



### 9.3 IMPACT ON CRISIS STABILITY

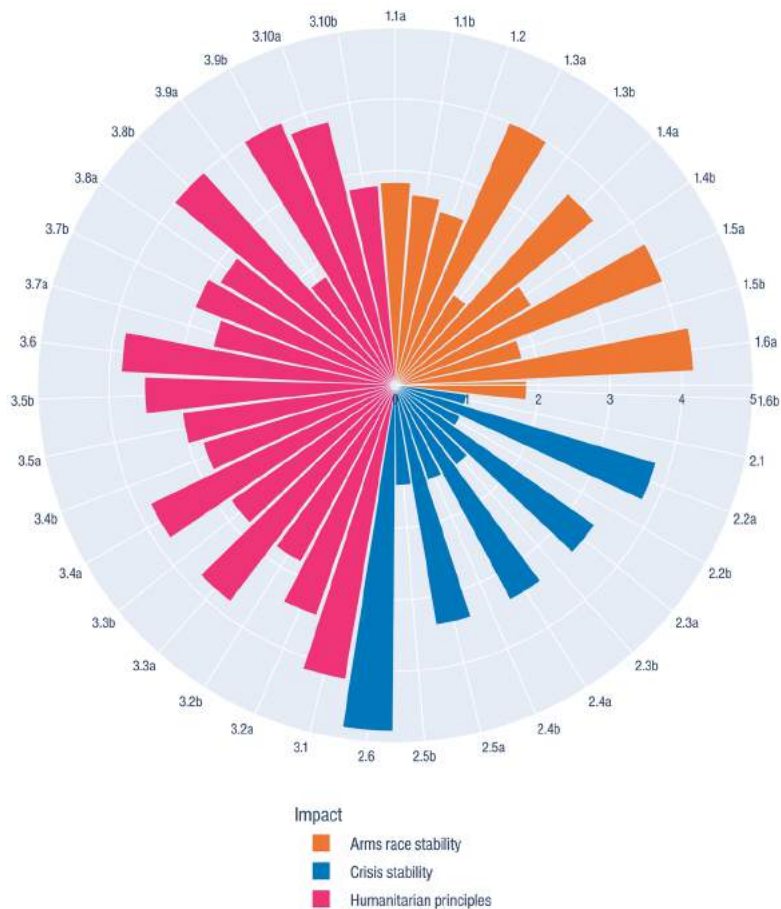
**The impact of DEWs will depend on the target.** Experts suggested that DEWs could impact crisis stability if states use them to deny adversary missiles, damage or degrade satellites, or ‘soak up’ retaliation after a kinetic first strike. Many experts discussed their ability to degrade NC3 and ISR, noting that DEWs could ‘blind’ or destroy sensors, early warning, and space-based communication links. One expert implied that this could pose a threat to Russia’s ability to execute launch on warning, which could increase its reliance on automated or semi-automated elements within its NC3 architecture. Another expert noted that high-powered microwave payloads on cruise missiles, which experts claimed are currently under development in the United States, could facilitate a strike designed to cripple power grids or disable command centres, to name two potential targets. Finally, targeting some combination of communication links and personnel could decrease decision making time and situational awareness, while reducing the availability and quality of information during a crisis.

### 9.4 IMPACT ON HUMANITARIAN PRINCIPLES

**This technology could help strengthen compliance with the principle of proportionality, but could also create attribution challenges.** According to experts, the accuracy of this technology presents opportunities to reduce collateral damage. Experts cited the non-lethal utility of DEWs as another potential benefit in situations where civilians are present (e.g., for crowd control or reversible electronic attacks on civilian vehicles), where this technology may be utilised as a more humane option. On the other hand, it may prove difficult for the targeted side to establish the existence and source of a directed energy attack (e.g., microwave radiation). According to one expert, the challenges associated with attribution could result in aggressors using these weapons with impunity.

## 10 PHYSICAL HUMAN ENHANCEMENT TECHNOLOGIES

**Figure 10: Mean score per question – Physical human enhancement technologies**



### 10.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

The main barriers to the development of physical HET are ethical and technical. Physical HET cover a broad range of capabilities. Some are already well developed, whereas others are still at the conceptual stage. Experts anticipated that the United States would face ethical barriers to development, particularly in relation to the more controversial applications of physical HET

(e.g., significant neurological enhancement). The challenges for Russia, in contrast, are predicted to be primarily technical, with comparatively fewer ethical, social, and cultural constraints. Experts predicted that China would face fewer obstacles to development, both ethically and technically.

The main drivers of this technology relate to enhanced battlefield performance. According to experts, these are shared by the United States, Russia, and China. Physical HET could, depending on their application, improve soldier resilience, reduce the human cost of war, and create other battlefield advantages conducive to military effectiveness. Experts predicted that these features may be particularly attractive to states with smaller forces, who rely more heavily on combatant quality than quantity. Experts do not expect that the development of this technology will place too great a financial burden on the United States.

## 10.2 IMPACT ON ARMS RACE STABILITY

**Experts did not express a strong opinion on the potential of this technology to impact regional or arms race stability, either positively or negatively.** They did, however, note the potential difficulty of verifying and monitoring human enhancement and genetic modification, which could complicate future arms control agreements in this area.

## 10.3 IMPACT ON CRISIS STABILITY

**The impact of physical HET on crisis stability is expected to be mixed.** According to experts, physical HET could provide benefits during a crisis, enhancing the alertness of combatants and decision makers and enabling more streamlined information processing and responses. However, this technology also comes with risks. Experts warned that faster access to greater information flows through neural interfacing may result in greater uncertainty and an overreliance on computational decisions. Enhancements may also lead those impacted to overestimate their own capacity to comprehend information and react appropriately. This would be particularly detrimental in a crisis scenario, where compressed action timelines can generate or increase the likelihood and cost of errors in judgement.

## 10.4 IMPACT ON HUMANITARIAN PRINCIPLES

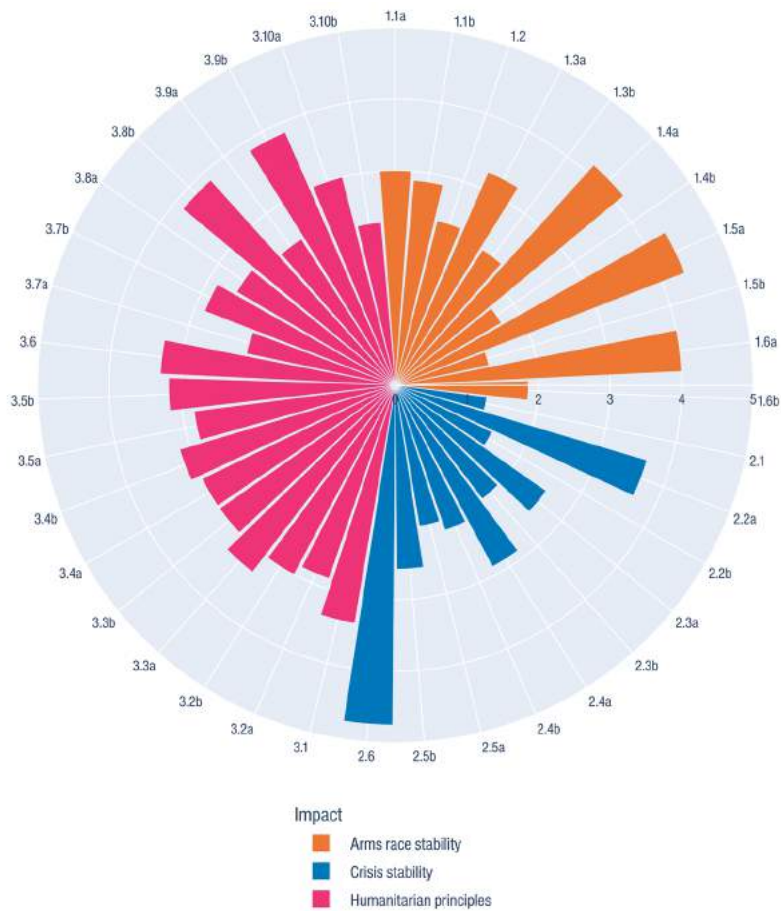
**Physical HET have the potential to both increase and mitigate civilian harm in war.** Any technology that enhances the health and alertness of combatants has the potential to improve compliance – or at least the possibility of compliance – with international humanitarian law. Experts noted this in relation to the principles of discrimination, proportionality, and precaution. Much will depend on the specific innovation, however. Experts highlighted that modifications that lead fighters to overestimate their abilities may incentivise misguided and reckless conduct. Likewise, modifications that enhance combatant aggression may have a deleterious impact on civilian protection.

**Physical HET also pose novel challenges to other humanitarian principles of war.** Experts highlighted the possibility that new divisions may open up on the battlefield between enhanced and un-enhanced humans. This would test a range of moral and legal assumptions related to inhumane treatment, prisoner of war status, and accountability. Experts also mentioned the possibility of harnessing this technology to erase, or mitigate the risk of, traumatic battlefield experiences.

**Physical HET may expose those affected to new vulnerabilities.** Experts noted that any modifications that are networked (e.g., via Bluetooth) would be susceptible to hacking and spoofing. This could pose an attribution challenge in the event of accidents or battlefield misconduct. Experts also questioned whether the physical modification of combatants and decision makers could undermine meaningful human control over targeting decisions in war.

## 11 COGNITIVE HUMAN ENHANCEMENT TECHNOLOGIES

**Figure 11: Mean score per question – Cognitive human enhancement technologies**



### 11.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

The main barriers to the development of cognitive HET are technical and ethical. While the United States, China, and Russia have made progress in the development of some enabling technologies (e.g., CRISPR), the brain is still poorly understood, and significant ambiguity exists regarding the viability of the more ambitious predicted effects of cognitive HET. Experts anticipate that the

United States, Russia, and China will likely face significant technical barriers to the application of this group of technologies. Experts also raised moral and ethical concerns that could arise at both the public and the political level, though experts anticipate that these could be less constrictive for Russia and China.

The possibility of enhancing human combatants and military decision makers in ways that improve battlefield performance and mitigate the costs of war was seen as an important driver for the United States, China, and Russia. Experts viewed the more comprehensive integration of humans and autonomous systems (e.g., via brain-computer interfacing) as another potential military advantage, as it could enable militaries to more fully capture the benefits that come from information processing and actioning at machine speeds. Experts did note, however, that perceptions of military advantage could outweigh the realities.

## 11.2 IMPACT ON ARMS RACE STABILITY

**This technology has the potential to both undermine and bolster arms race stability.** Experts did not anticipate that cognitive HET will have a significant impact on the military spending priorities of the United States in the short term. As military networks become increasingly intricate and autonomised, however, cognitive upgrades could offset the perception of humans as the weakest link in the action chain. Experts noted that this could have a positive impact on global and regional stability if such innovations allow for more accurate information communication and greater situational awareness.

**Experts warned that the drive to develop cognitive HET also has the potential to trigger an arms race and a ‘race to the bottom’,** with human experimentation intensifying in the absence of ethical and legal constraints. One expert predicted that of all the technologies examined in this study, cognitive HET have the highest likelihood of being universally outlawed, on account of their morally and legally problematic status. Other experts expressed concern regarding their potential to fall through the regulatory gaps or undermine existing arms control agreements. These concerns derive from the perceived difficulty of detecting the cognitive augmentation of humans.

### 11.3 IMPACT ON CRISIS STABILITY

**Augmented humans could conceivably improve NC3, with positive implications for crisis stability.** Experts noted potential benefits such as increased alertness, improved processing capacity under time and pressure constraints, and higher cognitive functioning.

**Experts also highlighted several risks related to cognitive HET and crisis stability.** ‘Enhanced’ humans will still be prone to miscalculation and bias and could operationalise these errors in ways that are less observable and preventable. Experts also reiterated the profound uncertainty surrounding the application of this group of technologies. There is still no consensus on which qualities (e.g., advanced reasoning, emotional intelligence, cool-headedness) militaries should value and foster in combatants and leaders within a crisis context. Enduring uncertainty over which qualities to promote and suppress in humans complicates predictions regarding decision making and the broader crisis implications of this group of technologies.

### 11.4 IMPACT ON HUMANITARIAN PRINCIPLES

**Improving the cognitive abilities of those who fight has the potential to improve compliance with battlefield rules.** Enhanced perception and faster information processing could, experts conceded, enable a more discriminate and proportionate application of violence that might better safeguard the lives of civilians. According to one expert, however, flawed brain-computer interfacing could also weaken essential restraints in war. Experts also pointed out that there may be a point at which human augmentation becomes so intensive that it calls into question the applicability of existing regulatory frameworks.

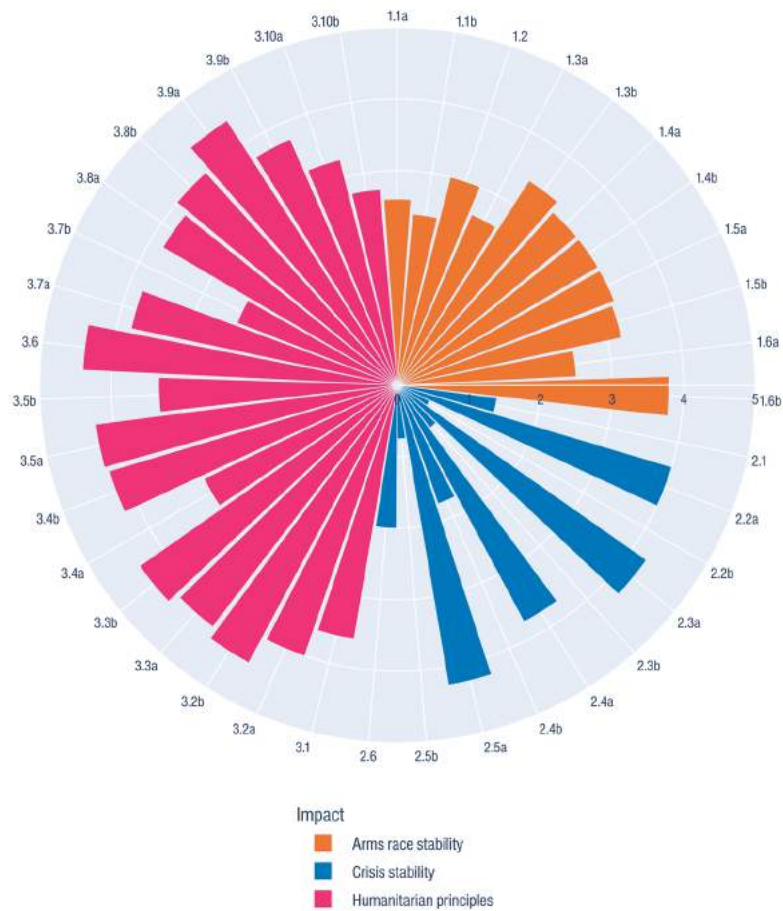
**Cognitive HET could generate several challenges in relation to humane treatment in war.** Experts highlighted the possibility that this technology could create new divisions on the battlefield between enhanced and un-enhanced humans. This would test a range of moral and legal assumptions relating to inhumane treatment, prisoner of war status, and accountability. Experts also noted the possibility of harnessing this technology to erase, or mitigate the risk of, traumatic battlefield experiences.

**Cognitive HET may expose those affected to new vulnerabilities.** Experts noted that any modifications that are networked (e.g., via Bluetooth) would be susceptible to hacking and spoofing. This could pose an attribution challenge in the event of accidents or battlefield misconduct. Experts also questioned whether the cognitive modification of combatants and decision makers could undermine meaningful human control over targeting decisions in war.



## 12 SYNTHETIC BIOLOGY

**Figure 12: Mean score per question – Synthetic biology**



### 12.1 MAIN BARRIERS TO AND DRIVERS OF TECHNOLOGY DEVELOPMENT

The main barriers to developing and deploying weaponised synthetic biology are the strong legal and normative restrictions against such conduct. The United States, China, and Russia are states parties to the Biological Weapons Convention (BWC). According to the experts, the United States is unlikely to develop biological weapons for explicit offensive purposes. Experts further

noted, however, that the BWC does allow for biodefence and that the line between the development of offensive and defensive applications in this area is ambiguous.

Beyond moral and legal concerns, experts emphasised technical challenges, particularly in relation to the collection of genomic, pathogen, epigenetic, and health data. Experts anticipated that Russia and China will struggle more than the United States in this area, on account of its less-developed private sector.

Broader societal and economic benefits (e.g., to health, agriculture, and manufacturing), as well as potential advantages on the battlefield, may drive the development of synthetic biology in the future. Experts regarded China as well positioned in many salient research fields, including biotechnology and genetic research, though the extent to which this translates into effective military capacity remains unclear. Experts also referred to Russia's long history of covert biological weapons development. If Russia opts to further develop this technology, it will likely be a credible player in this space. Finally, experts anticipated that the United States will devote more resources to this technology in the coming years.

## 12.2 IMPACT ON ARMS RACE STABILITY

According to the experts, **the proliferation of synthetic biology for military purposes by state and/or non-state actors would have profoundly destabilising effects.** The verification and monitoring of bioweapon development and deployment has always been challenging, and the international community may struggle to prevent the spread of synthetic biotechnologies. If violations of the BWC are not detected and punished, regulatory measures may be weakened. This, experts warned, could also have a spill-over effect, with the ultimate consequence of undermining broader commitments to arms control.

## 12.3 IMPACT ON CRISIS STABILITY

Experts did not anticipate that synthetic biology will significantly impact crisis stability.

## 12.4 IMPACT ON HUMANITARIAN PRINCIPLES

**The development and deployment of synthetic biology in a military context is likely to have severe humanitarian consequences.** Experts pointed out that biological weapons – particularly those that depend on contagiousness or transmissibility – are unable to be used in accordance with the principle of distinction. The difficulties associated with controlling the spread of such agents are likely to exacerbate civilian vulnerability and harm in both military and non-military settings. Experts also raised the issue of attribution: it may be difficult to determine the party responsible for releasing a modified virus. Experts cited the ongoing debate over the COVID-19 ‘lab leak’ theory to illustrate this difficulty. Finally, experts raised the possibility that synthetic biology attacks could be favoured as an alternative to more direct kinetic action.

## ABOUT THE AUTHORS

**Marina Favaro** is a Research Fellow in the 'Arms Control and Emerging Technologies' project at the IFSH. [favaro@ifsh.de](mailto:favaro@ifsh.de)

**Dr Neil Renic** is a Senior Researcher in the 'Arms Control and Emerging Technologies' project at IFSH. [renic@ifsh.de](mailto:renic@ifsh.de)

**Dr Ulrich Kühn** leads the project on 'Arms Control and Emerging Technologies' at IFSH. [kuehn@ifsh.de](mailto:kuehn@ifsh.de)

## ABOUT THE PROJECT

The research and transfer project 'Arms Control and Emerging Technologies' examines the status, functions, and strengthening of arms control, disarmament, and the control of emerging technologies. It is funded by the German Federal Foreign Office.

Funded by:



Federal Foreign Office

## ABOUT THE INSTITUTE

The Institute for Peace Research and Security Policy (IFSH) researches the conditions for peace and security in Germany, Europe and beyond. The IFSH conducts its research independently. It is funded by the Free and Hanseatic City of Hamburg.



Funded by:

Ministry of Science,  
Research, Equalities  
and Districts

DOI: <https://doi.org/10.25592/ifsh-research-report-010> Copyright Cover Foto: dpa Picture Alliance / Zoonar | Kheng Ho Toh

Text license: Creative Commons CC-BY-ND (Attribution/NoDerivatives/4.0 International).



**IFSH - Institute for Peace Research and Security Policy** at the University of Hamburg

Beim Schlump 83 20144 Hamburg Germany Phone +49 40 866077 - 0 [ifsh@ifsh.de](mailto:ifsh@ifsh.de) [www.ifsh.de](http://www.ifsh.de)