The Hague Centre
for Strategic Studies

Deterring or Spiralling?

Emerging Technologies, Strategic Stability, and Prospects for Sino-European Arms Control

Davis Ellison, Tim Sweijs and Timur Ghirotto

March 2025

The Hague Centre
for Strategic Studies

Deterring or Spiralling?

Emerging Technologies, Strategic Stability, and Prospects for Sino-European Arms Control

Authors:
Davis Ellison, Tim Sweijs and Timur Ghirotto

Contributors:
Ayla Elzinga, Julia Döll and Paul van Hooft

QA:
Frank Bekkers

March 2025

The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defense.

Table of Contents

Executive Summary

Emerging and disruptive technologies (EDTs) are set to negatively affect strategic stability in the coming years. From a European arms control perspective, it is critically important to turn shared concerns about the impact of emerging and disruptive technologies (EDTs) on strategic stability into momentum for progress on arms control initiatives, including with the People's Republic of China. China is currently both an EDT and a military powerhouse that is adapting its nuclear posture and expanding its nuclear arsenal. In the context of Sino-American competition, Europeans will need to engage with China. Doing so in a bilateral format between China and European states, or the EU itself for that matter, is already quite a challenge. The current policy direction pursued by various European states towards the Indo-Pacific makes engagement difficult from Beijing's perspective. However, if European states are concerned about being associated with what is likely to be a highly aggressive stance from Washington towards China, it would be logical to also engage with Beijing directly on areas of mutual concern.

In the context of Sino-American competition, Europeans will need to engage with China.

The discussion on EDTs in relation to nuclear weapons is often both alarmist and unspecific. It envisages a *Skynet*-style future in which nuclear weapons can be launched without human intervention, *à la* the third Terminator film. This alarmism can obscure more meaningful study of the pathways through which new technologies affect strategic stability. Assigning future risk estimates is difficult because of epistemic uncertainty associated with both the nature of these technologies, the way in which actors will deploy these technologies, and how this in turn is perceived by other actors.

There are, at the same time, real risks associated with the maturation and adoption of these new technologies. EDTs can reduce the ability of an adversary to maintain a secure nuclear second-strike capability and thereby undermine strategic stability. First, decision makers could surmise that a first strike would be highly effective. This can drive a process of armament and lead them to assume a more forward leaning, aggressive strategic posture (deterrence stability). In the context of a crisis, it may also engender use-them-or-lose-them dynamics (crisis stability). Second, the opposite party could conclude that its adversary is aggressively pursuing these technologies with the aim of preparing for a first strike creating similar escalatory spirals. This report examines this connection in detail, beginning with a review of past discussions on damage limitation strategies and the attendant risk to strategic stability.

In doing so, this report considers three pathways through which EDTs affect strategic stability in relation to EDTs, specifically by 1) enabling a first strike, 2) enabling the disruption of command-and-control systems, and 3) enabling the defence of a secure second-strike capability. These pathways emerge from the general literature on nuclear strategy and strategic stability, and more specifically from the logic of damage limitation that has become particularly salient in this era of heightened instability. As for the specific EDTs, the report assesses the impact of hypersonic missiles, cyber, directed energy, space, and artificial intelligence (AI). These have been selected for their specific applicability to strategic stability. Additionally, hypersonics, space, and AI are all already EDT focus areas for NATO, and therefore relevant for European defence.

Strategic Tasks

Offence	First Strike/Counterforce	The ability to initiate a rapid disarming attack in response to warning of attack
	'Bolt from the Blue'	The ability to initiate a no-notice offensive with the aim of quick defeat
C3 Disruption	Targeting and Analysis	Disrupting an adversary's ability to target their assets and analyse incoming attacks
	Deception Measures	Physical and non-physical measures to deceive adversary ISR
	Disrupting Communications	Kinetic and non-kinetic measures to disable adversary communication and early-warning systems
Defence	Delegation of Authorities	Ensuring prompt second-strike by delegating launch authority lower down chains of command, possibly to non-human systems
	Concealing Assets	Physical and non-physical measures to hide assets from detection
	Protecting Assets	Defence of targets through varieties of missile defence

What this report establishes, corroborated with both international expert opinion and reviews of Western and Chinese literature, is that there is mutual concern, perhaps concern sufficient to support momentum towards risk reduction measures and increased transparency between European states and China. Rapidly pursuing and fielding EDTs that imply an attempt to achieve a disarming, first-strike advantage can only serve to accelerate spiral dynamics instead of bolstering deterrence. A supplement to this report explores possible arms control pathways in greater detail, but understanding the impacts of these new technologies on stability underpins the following arms control considerations:

- **Build on shared concerns in space.** Space as a global common is at great risk in the event of war. Targeting or interfering with space-based early-warning, nuclear command and control infrastructure, or communications systems risks not only serious miscalculation and escalation, but also creating debris fields that make space less usable for all. This shared impact and concern is a platform from which dialogue can be pursued.
- **Consider areas of unilateral restraint, particularly when it comes to AI-enablement.** Imposing limits on the integration of AI-applications into military systems, especially those related to decision-making involving the use of force, will be an important area to signal cooperative intent towards Beijing.
- **Be transparent about the aims of hypersonic development.** The development and testing of hypersonic technology is fraught with opportunities for misunderstanding. To some observers, it communicates an aim to pursue a first strike strategy. For Europeans, this would not only be quixotic due to the size of the Russian arsenal, but also destabilising and only exacerbate arms racing tendencies. It is therefore necessary to be as transparent as possible concerning the concepts of operations and doctrines that these weapons underpin in order to reduce misperceptions.
- **Consider closer nuclear consultation ties with France and the UK.** The existing 'iron triangle' of defence agreements between Paris, London, and Berlin (the treaties of Lancaster House, Aachen, and Trinity House) provide for a strong level of consultation on defence planning and priorities. These treaties could open the door for more frameworks outside of NATO to propose meaningful dialogue measures with other states. France and the UK, as Europe's independent nuclear powers, have a vital voice in any possible arrangements.
- **Maintain European-Chinese dialogue at the Track 1.0, 1.5, and 2.0 levels.** Dialogue with China through the upcoming Trump administration is risky given the possibility of retaliation from Washington. However, as part of establishing an independent negotiating position on EDTs, channels with Beijing should be kept open across levels, with the objective to institutionalise these interactions outside the narrative of Sino-American competition.

1. Introduction

Is Europe running headlong into a high-tech arms race with China? Is this creating a risk of war? The discussion on emerging and disruptive technologies (EDTs) in relation to nuclear weapons is often both alarmist and unspecific. It envisages a *Skynet*-style future in which nuclear weapons can be launched without human intervention, *à la* the third Terminator film. This alarmism can obscure more meaningful study of the pathways through which new technologies affect strategic stability. Assigning future risk estimates is difficult because of epistemic uncertainty associated with both the nature of these technologies and how actors will put these technologies to use, and with how this is perceived by other actors.

1.1. The Impact of EDT on strategic stability

Nuclear-armed great powers run tremendous risks when they engage in direct confrontations with each other.

In this report we take a more schematic look at EDT. We focus on classic strategic stability concepts including crisis and deterrence stability and how these may be affected through the impact of EDT on first strike, second strike and damage limitation. There is a significant extant literature on these topics, refined over the course of the Cold War and revisited over the decades since as new nuclear powers emerged, technology advanced, and global tensions ebbed and flowed.[1] Importantly, we acknowledge and incorporate the argument that EDT-enhanced conventional weapons could advance to the point of reaching nuclear-level effects, something noted not only by analysts but even in state nuclear doctrines.[2] Our overall analysis and discussion is approached with caution, given how difficult it is to understand nuclear dynamics in the absence of a larger empirical evidence base. We recall American RAND strategist Alain Enthoven's oft-quoted statement, "General, I have fought just as many nuclear wars as you have," and preface that this report by necessity strays into abstraction.

With the advent of nuclear weapons, nuclear-armed great powers run tremendous risks when they engage in direct confrontations with each other. American political scientist Robert Jervis, among others, argued that this so-called nuclear revolution would significantly dampen the risks of great power war,[3] even if 'power politics' undisputably have continued 'in the Atomic Age'.[4] The essential condition is that nuclear-armed states have a secure second strike, so that they cannot disarm each other's arsenal. In other words, a secure second strike

1 Lawrence Freedman and Jeffrey Michaels, *The Evolution of Nuclear Strategy: New, Updated and Completely Revised*, 4th ed. 2019 edition (London: Palgrave Macmillan, 2019).

2 Tom Sauer, 'The Potentially Revolutionary Impact of Emerging and Disruptive Technologies and Strategic Conventional Weapons on the Nuclear Deterrence Debate', Non-Proliferation and Disarmament Papers (Brussels: EU Non-Proliferation and Disarmament Consortium, December 2024), https://www.nonproliferation.eu/wp-content/uploads/2024/12/EUNPDC-no_91.pdf; Fabian Hoffmann and William Alberque, 'Non-Nuclear Weapons with Strategic Effect: New Tools of Warfare?' (London: International Institute for Strategic Studies, March 2022), https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2022/03/non-nuclear-weapons-with-strategic-effect-new-tools-of-warfare.pdf.

3 Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Cornell University Press, 1989).

4 Keir A. Lieber and Daryl G. Press, *The Myth of the Nuclear Revolution: Power Politics in the Atomic Age*, Cornell Studies in Security Affairs (Cornell University Press, 2020), https://www.jstor.org/stable/10.7591/j.ctvqc6jj1.

ensures that they can always retaliate against their adversary, even after a nation-destroying attack. New technologies that put second strike capabilities at risk will therefore have a profound impact on strategic stability.

There are five strategies to secure a second-strike capability: redundancy, concealment, mobility, hardening, and loosening command and control through so-called delegation. States can choose redundancy and build up an arsenal too large to destroy in one go. They can try to keep their delivery systems concealed and mobile, through such means as submarines, aircraft, and mobile launchers. They can harden their silos, if they have them, to survive direct attacks. Finally, they can change their posture to loosen the criteria for launch.[5] These means are imperfect however, given the targeting abilities of advanced adversaries such as Russia and China. There is no such thing as an invulnerable second-strike. Policymakers are uncomfortable accepting these vulnerabilities, especially US leaders.[6] Instead, they pursue damage limitation strategies, either through the targeting of enemy nuclear assets or through enhanced ballistic missile defence (or both) with which they can decrease that vulnerability. These damage limitation strategies undermine the stability of the nuclear revolution in which political and military leaders in nuclear powers have frequently reiterated that nuclear war cannot be won and must never be fought. The combination of the logic of damage limitation with the applications of new technologies is where risk begins to emerge because of interaction effects that undermine the foundations of strategic stability, as we will explain in this report.

EDTs can reduce the ability of an adversary to maintain a secure second-strike and risk stability in two ways. First, a decision maker could surmise that a first strike would be highly effective with more advanced weapons systems and enablers. This can drive a process of armament and lead them to assume to a more forward leaning, aggressive strategic posture (risking deterrence stability). In the context of a crisis, it may also engender use-them-or-lose-them dynamics (crisis stability), where nuclear use becomes desirable. Second, the opposite party could conclude that its adversary is aggressively pursuing these technologies with the aim of preparing for a first strike creating similar escalatory spirals by incentivising a preventive attack.[7] This report explores this connection in detail, beginning with a review of past discussions on damage limitation strategies and the attendant risk to strategic stability.

On this basis, this report then looks at three aspects of strategic stability in relation to EDTs. Each is used to explore how new technologies can impact stability in practice, specifically by:

1. enabling a first strike;
2. enabling the disruption of command-and-control systems; and
3. enabling the defence of a secure second-strike capability.

---

5 Davis Ellison and Paul van Hooft, "Good Fear, Bad Fear: How European Defence Investments Could Be Leveraged to Restart Arms Control Negotiations with Russia" (The Hague, The Netherlands: The Hague Centre for Strategic Studies, 2023), https://hcss.nl/report/good-fear-bad-fear-how-european-defence-investments-could-be-leveraged-to-restart-arms-control-negotiations-with-russia/.

6 Brendan Rittenhouse Green, *The Revolution That Failed: Nuclear Competition, Arms Control, and the Cold War* (Cambridge University Press, 2020); Keir A. Lieber and Daryl G. Press, *The Myth of the Nuclear Revolution: Power Politics in the Atomic Age* (London: Cornell University Press, 2020), http://www.jstor.org/stable/10.7591/j.ctvqc6jj1.

7 Morgan, Forrest E., Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff. "Dangerous Thresholds: Managing Escalation in the 21st Century." RAND Corporation, July 8, 2008. https://www.rand.org/pubs/monographs/MG614.html.

These pathways emerge from the general literature on nuclear strategy and strategic stability, and more specifically from the logic of damage limitation, a strategy that has become particularly salient in an era of heightened geopolitical instability. As for the specific EDTs, we focus on hypersonic missiles, cyber, directed energy, space, and artificial intelligence (AI), each of which is considered in reference to the three aspects above. These EDTs have been selected for their specific applicability to nuclear operations. Additionally, hypersonics, space, and AI are all EDT focus areas for NATO, and therefore relevant for European defence.

1.2. EDT, strategic stability, and the prospects for Sino-European engagement

The dynamics explored in this report are particularly important in relation to China, given that Beijing has until now remained outside most arms control measures other than the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and is one of the leading military technology forces in the world. The possibilities of building new confidence and security building measures (CSBMs) for emerging technologies are a potential pathway towards some level of transparency, if not stability, with Beijing. There are, however, important differences to consider when drawing on past historical experience.

China is not the Soviet Union, and we should not draw too heavily upon the Cold War as precedent. China is "an increasingly wealthy and technologically advanced country capable of engaging…in sustained, sophisticated nuclear competition."[8] This new competition is not simply about greater spending, as China cannot simply be outspent. Furthermore, for all its modernisation, Beijing does not invest at the near-suicidal rate of Soviet military spending of roughly 15-17% of gross national product. China's current rate sits at just short of 2%, according to SIPRI.[9] China has additionally identified a series of areas where EDTs can be best leveraged to develop conventional systems with strategic effects that could deter nuclear attack by the US.[10]

Further, China's quantitative growth in nuclear weapons creates a multipolar deterrence dilemma for Europe's nuclear powers, the UK and France. US extended deterrence in Europe is coming under pressure as Washington plans for contingencies with Russia, China, and North Korea simultaneously, especially since the incoming Trump administration is quite likely to favour the policies of damage limitation discussed earlier in this study. As the US works to enact these strategies against multiple opponents, this puts both nuclear advocates and opponents in Europe in a difficult spot. The US will have fewer nuclear assets to commit to European defence just as it continues to step away from arms control as a policy preference.[11]

---

8 Charles L. Glaser and Steve Fetter, 'Should the United States Reject MAD? Damage Limitation and U.S. Nuclear Strategy toward China', *International Security* 41, no. 1 (2016): 49–98.

9 'China - SIPRI Military Expenditure Database', Stockholm International Peace Research Institute, accessed 6 December 2024, https://milex.sipri.org/sipri.

10 Fiona Cunningham, *Under the Nuclear Shadow: China's Information-Age Weapons in International Security* (Princeton, N.J: Princeton University Press, 2025).

11 Alexander Mattelaer, 'China's Nuclear Shadow Reaches Europe' (London: Royal United Services Institute, 8 October 2024), https://www.rusi.org/explore-our-research/publications/commentary/chinas-nuclear-shadow-reaches-europe; Linde Desmaele, 'US Security Assurances and Nuclear Tripolarity', *Survival* 66, no. 2 (3 March 2024): 143–56, https://doi.org/10.1080/00396338.2024.2332066.

Europe is increasingly on its own when it comes to matters of arms control and its relationship to defence policy.[12]

Why has China largely excluded itself from many global arms control arrangements, particularly those that are most applicable to EDTs like the Wassenaar Arrangement or the Missile Technology Control Regime (MTCR)? First and foremost is a perceived hostility from Washington, a perception that is distinctly difficult for the United States to counter given its military posture in the region and its now entrenched strategy of containment of China.[13] US pursuit of advanced systems poses precisely the risks to deterrence stability discussed in the section above and throughout this study. The second is that China is a significant arms exporter itself with a significant domestic defence industrial base. Though much of China's exports do not fit within the EDT categories included in this assessment, joining broader agreements could negatively impact Chinese defence industry and would thus be undesirable.

The trick will be to turn shared concerns about emerging technologies and strategic stability it into momentum for arms control measures.

A bare minimum foundation for productive dialogue is the shared recognition between European states interested in such discussions and Beijing that the EDTs above are increasingly challenging strategic stability around the world. This is seemingly the case, with a wealth of publications from European and Chinese authors on this topic highlighting the risks such technologies pose. There are, however, crossed purposes when it comes to even the most preliminary outcomes. For example, at the September 2024 Summit on Responsible AI in the Military Domain (REAIM) conference in Seoul, Beijing did not sign the blueprint for action that was agreed by over 60 other countries.[14] This is not particularly surprising, given Beijing's consistent stance that arms control measures in these areas are part of a U.S. attempt to prevent its military rise, but disconcerting nonetheless.[15] Still, there has already been some progress, for example in the November 2024 US-China pledge to ensure AI would not replace human control over nuclear weapons, a statement that itself builds upon a joint US-UK-French position submitted in the 2022 NPT Preparatory Committee.

Fundamentally, the trick will be to turn shared concerns about emerging technologies and strategic stability it into momentum for arms control measures. This begins with transparency. The OSCE Vienna Document provides some precedence for this in the European case with Russia, with information exchanges on military research and development programmes being a possible measure.[16] Doing so in a bilateral format between China and European states, or the EU itself for that matter, is a challenge. The current policy direction pursued by various European states towards the Indo-Pacific makes engagement difficult from Beijing's perspective. In the Dutch example alone, the deployment of the *Tromp* frigate in the summer of 2024 prompted a militarised response from the PLA, with the Chinese air forces harassing

12 Paul Van Hooft and Davis Ellison, 'Good Fear, Bad Fear: How European Defence Investments Could Be Leveraged to Restart Arms Control Negotiations with Russia' (The Hague, Netherlands: Hague Centre for Strategic Studies, 2023).

13 Tong Zhao, 'Underlying Challenges and Near-Term Opportunities for Engaging China', *Arms Control Today* (blog), February 2024, https://www.armscontrol.org/act/2024-01/features/underlying-challenges-and-near-term-opportunities-engaging-china.

14 Joyce Lee, 'Sixty Countries Endorse "blueprint" for AI Use in Military; China Opts Out', *Reuters*, 10 September 2024, sec. Artificial Intelligence, https://www.reuters.com/technology/artificial-intelligence/south-korea-summit-announces-blueprint-using-ai-military-2024-09-10/.

15 Tong Zhao, 'The Real Motives for China's Nuclear Expansion', *Foreign Affairs*, 3 May 2024, https://www.foreignaffairs.com/china/real-motives-chinas-nuclear-expansion; Christopher S. Chivvis, 'U.S.-China Relations for the 2030s: Toward a Realistic Scenario for Coexistence' (Washington, D.C.: Carnegie Endowment for International Peace, October 2024), https://carnegieendowment.org/research/2024/10/us-china-relations-for-the-2030s-toward-a-realistic-scenario-for-coexistence?lang=en.

16 'Vienna Document on Confidence- and Security-Building Measures' (Organisation for Security and Cooperation in Europe, 2011), https://www.osce.org/files/f/documents/a/4/86597.pdf.

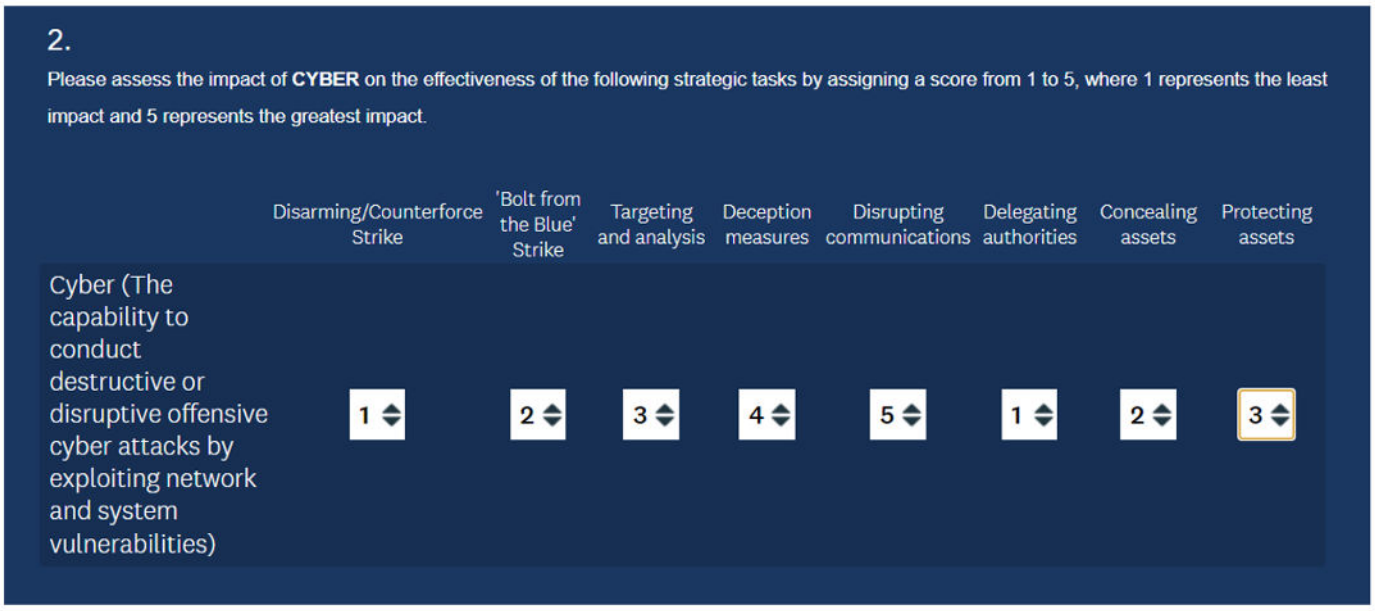
the frigate as it transited the East China Sea.[17] If European states are concerned about being associated with what is likely to be a highly aggressive stance from Washington towards China, it would be logical to engage with Beijing on areas of mutual concern. This report seeks to contribute to this endeavour outlining opportunities for Sino-European engagement in the sphere of EDT and strategic stability.

1.3. A note on method

This report has primarily relied on desk research conducted over the course of 2024, with sources including both the best, publicly available primary sources from states on military developments as well as secondary scholarly sources on strategic stability and EDTs. To buttress this research, HCSS conducted an international survey of experts in this field from different regions who were asked to rank the relative impacts of different technologies on strategic stability through various strategic missions.

The survey queried twenty five international security experts, specifically those working on strategic stability, deterrence and disarmament, to gauge expert opinion on the relative impact of the EDTs. Experts from Europe, North America, South Asia, East Asia, and South Africa, ranked the five EDTs (hypersonics, cyber, directed-energy weapons, space, and AI) from 1 to 5 to score their impact on stability, with 1 being the lowest and 5 the greatest impact. (see Figure 1 below for an illustration) The percentages reported in the study are the rate of respondents listing that EDT as either a 4 or 5.

Figure 1 The expert survey



[17] Seong Hyeon Choi, 'China Warns against Dutch Naval "Intrusion", Disputes East China Sea Encounter', *South China Morning Post*, 11 June 2024, https://www.scmp.com/news/china/diplomacy/article/3266181/china-warns-against-dutch-naval-intrusion-disputes-east-china-sea-encounter.

This report also benefited from a discussion of its main ideas, particularly related to arms control, at the Responsible Artificial Intelligence in the Military Domain Conference in Seoul in September 2024, at which a panel of South Korean, Indian, American, and European experts was convened. The main ideas of the conclusions here related to confidence and security building measures (CSBMs) were discussed at length, including the possibilities China's willingness to participate in such discussions. The arguments presented here have thus been exposed to a breadth of expert opinion possible, both in survey and in person formats.

The report begins with a discussion of the literature on the logic of damage limitation and the attendant measure-countermeasure competition that such a strategy propels. Following this, each of the three pathways is explored in turn, highlighting developments across the five EDT areas that are considered to be of most concern for strategic stability. It then concludes with a final assessment of the impact of EDTs on stability and implications for arms control, specifically those areas most relevant to future Sino-European engagement on these issues.

2. Offence, counter-measures, and arms racing logic

This chapter sets out the logic and tenets that form the basis for this reports analysis. It provides an overview of deterrence versus crisis instability. It reviews the logic of offensive nuclear strategies, followed by a consideration of the measure-countermeasure competition that the pursuit of such strategies engenders. The push and pull between offensive and defensive operations (specifically, missile launches and defence against them), along with attacks on the command, control, and communications (C3) systems enabling both, is dominated by the pursuit of specific EDT enhancements to technologies to try to gain an edge in any of the three tasks. Accordingly, the chapter ends by building on this logic and proposing a framework for categorising EDTs, with an aim to identifying those that are particularly destabilising.

2.1. The logic of the offensive and risks to strategic stability

Vulnerability is unattractive to policymakers.

Deterrence and crisis stability are interrelated concepts, both aiming to prevent either the outbreak or escalation of war through distinct logics. Deterrence is focused on discouraging aggression by convincing potential adversaries that the costs of an attack outweigh the benefits, primarily through the threat of assured retaliation. During the Cold War, the U.S. and Soviet Union maintained nuclear arsenals capable of mutual destruction for this precise purpose. Crisis stability, on the other hand, refers to the ability of nuclear states to avoid escalation during a tense situation. The Cuban Missile Crisis, again with the US and Soviet Union was an example of maintaining crisis stability despite immense pressure. Importantly, crisis stability as a concept also applies once a conventional war has started and parties seek to avoid this escalation of the conflict to the nuclear level. While deterrence seeks to prevent conflict by maintaining credible threats, crisis stability emphasizes the management of immediate risks to avoid unintended escalation. At the core of both concepts is a certain level of mutual vulnerability.

This vulnerability is unattractive to policymakers for obvious reasons. If they can limit the damage of an adversary's nuclear attack, they would prefer to do so. If they can entirely neutralise it, even better.[18] Such is the straightforward argument of a damage limitation strategy. There are three strategies available to states that pursue damage limitation. They can attack the adversary's nuclear arsenal before it can launch (including through non-kinetic 'left of launch' approaches). They can defend against the weapons that have been launched, through missile defence. And they can disrupt the adversary's ability to give the command to launch. Increasingly, more militarily advanced states pursue these three simultaneously.

[18] Matthew Kroenig, *The Logic of American Nuclear Strategy: Why Strategic Superiority Matters* (Oxford University Press, 2018).

Critics of damage limitation over the decades have argued that the strategy, and the technological pursuits to achieve it, both undermines deterrence by communicating a hostile intention and is technologically unfeasible. It is simply less credible for the United States, for example, to position itself as defensive in its military posture when it invests in acquiring new and modernising existing nuclear systems targeted against adversaries against which it already has a favourable nuclear and conventional balance. Further, it does begin to stray into "madman theory" territory when nuclear strategists begin negotiating between the deaths of millions versus tens of millions, particularly given the after-effects of nuclear weapons.[19]

From the military-strategic perspective, such a strategy is mainly concerned with land- and air-based nuclear threats. The survivability, and increased lethality, of nuclear-armed submarines undermines a damage limiting counterforce strategy as targeting these submarines is so difficult. Given that, for example, the Chinese JL-3 submarine-launched ballistic missile (SLBM) can carry a warhead ranging from 250-1,000 kilotons, the value of a limitation argument begins to decrease as more and more SLBMs continue to land on targets. Should such a "limited" exchange escalate to a countervalue, "city-trading" policy, the argument becomes even less tenable. Damage limitation starts to make little sense once tens of millions have died. Furthermore, missile defence becomes more difficult with SSBNs as they sneak closer to an enemy's coast and there is reduced time for an interceptor to launch. This has been balanced, however, with arguments that should anti-submarine warfare capabilities advance to such an extent that SSBNs can be more readily found and attacked, second-strike survivability could be reduced.[20]

Still, damage limitation remains the choice of many leaders given the political difficulty of making the argument that mutual vulnerability makes war less likely.[21] Furthermore, threat assessments can become skewed as states' military and intelligence officials consistently argue that the threat picture is worsening and is likely to deteriorate further in the future. This is particularly the case for militarily powerful states. As formulated by historian Andrew Bacevich, "the services have come to view outright supremacy as merely adequate."[22] This quixotic pursuit of unassailable military advantage is found time and again in Paul Kennedy's work *The Rise and Fall of Great Powers*, where Kennedy notes that in order to sustain its advantages, such as nuclear predominance, a large state will likely "find itself spending much *more* on defence than it did two generations earlier, and yet still discover that the world is a less secure environment."[23] Such a paradoxical outcome is one of the primary concerns of critics of nuclear modernisation and arms racing more generally and is precisely the outcome this report seeks pathways to avoid.

Damage limitation involves different tasks but generally involves offensive capabilities such as missiles in combination with efforts to disrupt enemy C3 systems. These capabilities can be targeted mainly at enemy nuclear capabilities, hence the idea of limiting damage from incoming nuclear weapons but taken to its extreme it can become a wider 'bolt from the blue' attack against a much broader target set, with the aim being to completely knock out an adversary's government and military in a surprise attack. These tasks, and how EDTs enhance them, is

19 Glaser and Fetter, 'Should the United States Reject MAD?'; George E. Lowe, 'Damage Limitation: A New Strategic Panacea?', *Proceedings* 91, no. 6 (June 1965): 7–48.

20 B.W. Bahney and B. Soper, 'The Delicate Balance Redux: The Role of Nuclear Forces, Damage Limitation and Uncertainty in Future U.S.-China Crises' (Livermore, CA: Lawrence Livermore National Laboratory, n.d.), https://cgsr.llnl.gov/sites/cgsr/files/2024-10/im-1098914-3.pdf.

21 Matthew Kroenig, *The Logic of American Nuclear Strategy: Why Strategic Superiority Matters*, Bridging the Gap (Oxford: Oxford University Press, 2018).

22 Andrew J. Bacevich, *The New American Militarism: How Americans Are Seduced by War* (Oxford: Oxford University Press, 2013), 18.

23 Paul Kennedy, *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000* (London: William Collins, 1988), 26.

explored in chapters three and four. Naturally, fears of such attacks feed a cycle of attempts to build countermeasures against these first strike weapons. This is explored in the section below, and the role of EDTs in this countermeasure competition is described in chapter five.

Investments in a new military technology have always led to investments in pursuit of a countermeasure.

2.2. Measure and countermeasure competition and arms racing

Investments in a new military technology have always led to investments in pursuit of a countermeasure.[24] This is as true for building better shields and taller castle walls as it is for space-based missile defence and AI-driven offensive cyber capabilities. It is nearly as assured as Newton's third law of motion, that for every action in nature there is an equal and opposite reaction. In military affairs, such competitions are endemic. Hardened bunkers bred 'bunker buster' bombs. Improved radars bred stealth aircraft. ICBMs have bred a continuous attempt to build missile defence shields. This type of competition became particularly intense during the Cold War. Efforts to preserve nuclear deterrents while trying to eliminate an opponent's led to the development of nuclear triads, heavy investment in missile defence technologies, massive civil defence construction projects, and the qualitative and quantitative improvement of individual weapons classes. (see the Textbox below for an example of the F117 Nighthawk)

Textbox: Measures and countermeasures: the case of the F-117 Night Hawk.

The development of the first stealth bomber, the F-117 *Nighthawk* is a strong example of a past measure/countermeasure competition. The F-117 concept was born after the Vietnam War, where sophisticated Soviet surface-to-air missiles (SAMs) had downed US heavy bombers, and after the 1973 Yom Kippur war, in which similar systems inflicted heavy losses on the Israeli Air Force. A 1974 US Defense Science Board assessment wrote that in the case of a conflict in Central Europe, Soviet air defences would likely prevent NATO air strikes on many targets in Eastern Europe. The *Nighthawk* went on to become the first truly stealth aircraft, incorporating two-dimensional flat surfaces (to reduce the radar cross-section), a non-circular tailpipe, and remaining limited to sub-sonic speeds to prevent a detectable sonic boom. Used heavily during the Persian Gulf War, it was part of a new era in US military technology. Still, the aircraft was not invincible. During the NATO operations over the then Yugoslavia, particularly Kosovo in 1999, two *Nighthawks* were hit by anti-aircraft fire, with one being downed. This, alongside the maturing of the F-22 *Raptor*, led to the programme's shuttering.[25]

[24] Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton University Press, 2004), https://doi.org/10.2307/j.ctt7s19h.

[25] David C. Aronstein and Albert C. Piccirillo, *Have Blue and the F-117A: Evolution of the 'Stealth Fighter'* (Reston, VA: American Institute of Aeronautics and Astronautics, 1997).

The Cold War period also shows that arms control measures to slow a measure/counter-measure spiral is possible, as in the case of the Anti-Ballistic Missile (ABM) Treaty of 1972. Intuitively, it seems difficult to convince an adversary to *not* invest in a technology that is notionally entirely defensive and meant to reduce harm to their own population. However, given that ABM technology makes a secure second-strike more survivable (in theory), it is a sign that a state could be building the capability to conduct an unstoppable nuclear first-strike. Nevertheless, the US and the Soviet Union agreed to ban missile defence systems designed to shoot down strategic missiles which included ICBMs and SLBMs. There was an attempt in 1997 to extend this more broadly to include theatre-range missile defences, though this faced significant opposition in the US Senate. In December 2001, the US under the Bush administration withdrew from the treaty, arguing it needed new systems to defend against nuclear blackmail from a 'rogue state' in reference to a nuclear-armed North Korea, Iran, or Iraq. This led to the creation of the US Missile Defense Agency and a range of projects under the national missile defence (NMD) programme. The subsequent US ABM withdrawal then augured in the longer-term erosion of the US-Russian arms control regime.[26]

Zero sum dynamics in this sphere can easily cross the threshold into a spiralling arms race, wherein security is undermined rather than supported by accelerating military developments. Of course, as Charles Glaser has noted, not all arms races are bad. A build up in the face of an aggressive neighbour naturally demands a response. But a real concern here, in direct relation to states seemingly pursuing damage limitation strategies as well as accelerating the inclusion of EDTs into nuclear enterprises, is that it generates spiral dynamics that further undermines stability. This is when a state's attempt to maintain superiority or to placate domestic interests such as the arms industry undermines stability to the point where a military build-up risks war.[27] Turning now to the technology itself, we unpack the respective impact of EDTs on states' pursuit of various strategic missions, including first- and second-strike, as well as missile defence and other non-kinetic tasks, while considering in each case the impact on strategic stability.

New technologies change the calculus of both defenders and attackers, or, more precisely, the calculus of nuclear-armed states as both defenders and attackers. They are both concerned about their own secure second strike and seduced by the possibility of limiting the damage to their own societies. This has led to investments around the globe into the array of capabilities covered in this study: hypersonic weapons, cyber, space capabilities (satellite constellations and anti-satellite weapons), directed energy weapons (on earth and in space), and artificial intelligence. We discuss their impact on three overarching categories: offence, C3 disruption, and defence. Each of these could conceivably be, or currently are, being developed with a damage limitation logic in mind. By being able to find, strike, and destroy targets more quickly and accurately, states could become convinced that they can hold adversaries' nuclear arsenals at risk. Finally, given the importance of communication in the event of a crisis, technologies that can interfere with or distort the content of information could lead to serious miscalculations if time is short.

In the next chapters, we inventory how these EDTs affect the perceived ability to pursue damage limitation strategies – first strike, 'bolt from the blue' attacks, communications disruption, and protection – as well as second strike securing strategies – analysis,

---

26 Richard Dean Burns, *The Evolution of Arms Control: From Antiquity to the Nuclear Age* (New York: Rowman and Littlefield Publishers, 2013), 34–35.

27 Charles L. Glaser, 'When Are Arms Races Dangerous? Rational versus Suboptimal Arming', *International Security* 28, no. 4 (1 April 2004): 81–84, https://doi.org/10.1162/0162288041588313.

deception, delegation, deception and again, protection. (Table 1 provides a summary of the key concepts):

Table 1. Strategic tasks and their operational objectives across Offence, C3 Disruption and Defence.

Strategic Tasks		
Offence	First Strike/Counterforce	The ability to initiate a rapid disarming attack in response to warning of attack
	'Bolt from the Blue'	The ability to initiate a no-notice offensive with the aim of quick defeat
C3 Disruption	Targeting and Analysis	Disrupting an adversary's ability to target their assets and analyse incoming attacks
	Deception Measures	Physical and non-physical measures to deceive adversary ISR
	Disrupting Communications	Kinetic and non-kinetic measures to disable adversary communication and early-warning systems
Defence	Delegation of Authorities	Ensuring prompt second-strike by delegating launch authority lower down chains of command, possibly to non-human systems
	Concealing Assets	Physical and non-physical measures to hide assets from detection
	Protecting Assets	Defence of targets through varieties of missile defence

3. First strike and bolts from the blue: EDTs and offence

A disarming first strike depends on countering the second-strike securing strategies of the adversary. Put simply, you hit their nuclear sites before they can fire in return. Such an event is commonly referred to as a "bolt from the blue" attack. It is an un-warned, sudden, and aggressive approach.[28] This kind of attack requires a lot to go right. Among other factors like timing and weather, it requires technical capabilities in the following areas:[29]

- Increased detection capabilities to find concealed and mobile nuclear weapon delivery systems.
- Improved precision weapons to destroy mobile nuclear weapon delivery systems, as well as to destroy hardened targets.
- Increased need to avoid detection of preparation for a strike and to avoid the defence systems of the adversary it seeks to attack.
- Deliberately sow confusion about whether an attack is actually taking place to undermine defensive response.
- Finally, it requires a significant number of redundant systems to strike the same target more than once if needed.

Prior to conducting such an attack, there is a requirement for up-to-date intelligence on the target state's nuclear posture. Where are their nuclear-capable aircraft housed? The bomb/missile vaults? ICBM siloes, road-mobile missile launcher storage and concealment sites? Some are of course easier to track than others, most obviously the ICBM siloes which dot the more rural areas of the larger nuclear-armed states. SSBNs pose the greatest danger, as they are much more difficult to find. Against a state such as the U.S., Russia, or China, early-warning systems are near-assured to pick up an attempted bolt from the blue attack as well, making a surprise disarming first strike even less likely.

Somewhat similar to damage limitation, a first strike strategy aims to disarm an adversary as much as possible, with an aim to conducting such an overwhelming attack that they are not able to or no longer want to respond.[30] It essentially seeks to 'win' a nuclear war in a one round

---

28 Frank Nuno and Vaughn Standley, 'Bolt out of the Blue: Nuclear Attack Warning in the Era of Information and Cyber Warfare', War on the Rocks, 14 June 2018, https://warontherocks.com/2018/06/bolt-out-of-the-blue-nuclear-attack-warning-in-the-era-of-information-and-cyber-warfare/.

29 Van Hooft and Ellison, 'Good Fear, Bad Fear: How European Defence Investments Could Be Leveraged to Restart Arms Control Negotiations with Russia'.

30 Even Hellan Larsen, 'Deliberate Nuclear First Use in an Era of Asymmetry: A Game Theoretical Approach', *Journal of Conflict Resolution* 68, no. 5 (1 May 2024): 849–74, https://doi.org/10.1177/00220027231185154.

knockout attack. Practitioners have been sceptical about the risk of such a strike. Even at the height of Cold War tensions, policymakers have cautioned that such an attack would be reckless in the extreme, with the possibility of retaliation from SSBNs and enemy radars detecting incoming strikes making a first strike knockout almost impossible. Put in 1983 by former US CIA director Admiral Stansfield Turner, 'Since we do have an invulnerable deterrent force in this country that can level his country, I don't believe any Soviet leader could have the kind of confidence to start that sort of an attack.'[31] Fears of such a strike remain today, however, with the recent popular books noting that since the authority to launch a nuclear attack is in the hands of so few, with some being dictators such as Kim Jong-un, we cannot be certain enough that a state may someday attempt a first strike.[32]

3.1. Emerging technologies enabling a possible 'bolt from the blue' strike

3.1.1. Hypersonic weapons

Perhaps the quintessential first strike weapon of the 21st-century is the hypersonic missile.

Perhaps the quintessential first strike weapon of the 21st-century is the hypersonic missile, or more specifically the hypersonic glide vehicle (HGV) which can be fitted onto different rocket boosters. Capable of speeds ranging from Mach 10 to over Mach 25 (the fastest reportedly being the Russian *Avangard* HGV), they are more importantly more manoeuvrable than existing ballistic missile systems, making missile defence efforts more difficult. For example, the US Space Based Infrared System and Defense Support Program (SBIRRS) satellites provide initial missile warning and early tracking that determines the positions, trajectories, and signatures of the missiles.[33] This, however, is dependent on the normal ballistic trajectory of a missile. HGVs, by evading or reducing the initial detection provided by space-based early warning systems, shorten the amount of time decision-makers have to respond to a possible attack. Further, midcourse interception, difficult enough with ICBMs, would become even harder. Ground- and maritime-based radars, which confirm an incoming attack after an early-warning satellite detects a launch, may be less able to detect threats as HGVs fly lower, limiting line-of-sight radar systems.[34]

In a multipolar world, where hypersonic capabilities may proliferate to more states around the world, the risks to both deterrence stability and crisis stability are amplified. The introduction of such weapons into fragile deterrence relationships increases the likelihood of misperceptions and misjudgements, making pre-emptive actions more tempting. As more states acquire

31 'First Strike - Interview with Admiral Stansfield Turner and John Collins', *American Interests* (Washington, D.C.: WETA-TV, February 1983), Georgetown University Dean Peter Krogh Foreign Affairs Digital Archives Videos, https://repository.library.georgetown.edu/handle/10822/552552.

32 Annie Jacobsen, *Nuclear War: A Scenario* (London: Transworld Publishers, 2024).

33 Douglas M. Fraser, Frank Gorenc, and John S. Shapland, 'Hypersonic Defense Requires Getting Space Sensor System Right', 13 May 2020, https://www.realcleardefense.com/articles/2020/05/13/hypersonic_defense_requires_getting_space_sensor_system_right-full.html.

34 Roza, 'Why Hypersonic Missiles' Greatest Strength Also Makes Them Vulnerable', 2023. Kelley M. Sayler'Product Details IF11623', accessed 28 May 2024, https://crsreports.congress.gov/product/details?prodcode=IF11623.

these technologies, the strategic environment becomes more unstable, increasing the probability of rapid escalation.[35]

From a deterrence stability perspective, the threat of decapitation strikes weakens confidence in an adversary's second-strike capability.[36] The primary function of nuclear command, control & communications (NC3) systems are to ensure that even after a debilitating first strike, a state retains the ability to retaliate. If hypersonic missiles can disable these systems with little warning, the adversary's confidence in their retaliatory capability is significantly undermined. This creates powerful first-strike incentives, as states may believe that striking pre-emptively is their only option to avoid total incapacitation of their nuclear forces.[37] Such a dynamic destabilises deterrence by making pre-emptive action more likely.

In crisis stability terms, hypersonic missiles targeting leadership or NC3 systems introduce extreme pressure on decision-making timelines.[38] The fear of losing the ability to communicate with or control nuclear forces can lead to hasty decisions and escalate tensions rapidly. The perceived threat of a decapitation strike could trigger use-it-or-lose-it dynamics. The compressed timeline for decision-making, combined with the complexity and speed of hypersonic missiles, significantly increases the risk of miscalculation and miscommunication, driving crisis instability.[39]

Combined with other emerging technologies, such as an AI-enabled guidance system that improves the strike's precision alongside its speed and manoeuvrability, heightens the challenge. Noted by Shah, "The faster and more accurate delivery platforms like hypersonic missiles, combined with advanced AI algorithms, will generate a greater sense of confidence in a state's ability to strike first."[40] It is quite arguable that the difficulty in tracking and intercepting more precise hypersonic weapons encourages retaliation before the first strike arrives and increases the likelihood of the adoption of a "launch-on-warning posture" or pre-emptive strike policy, a posture reportedly maintained by the United States as of this writing.[41]

3.1.2. **Cyberweapons**

Long-running debates have been had about the impact of the cyber domain on strategic stability. For many years, this was hampered by a lack of information regarding the 'cyber-weapons' state militaries and intelligence services operate. Since approximately 2018, however, more has become available through journalists' efforts and freedom of information requests regarding what operations and capabilities exist. It is clear at this stage that many major state actors have the capacity to at least attempt cyberattacks against adversary

35 Paul van Hooft, Lotje Boswinkel, and Tim Sweijs, "Shifting Sands of Strategic Stability: Towards a New Arms Control Agenda" (The Hague, Netherlands, 2022), https://hcss.nl/report/arms-control-shifting-sands-of-strategic-stability/.

36 Kelley Sayler M., 'Hypersonic Weapons: Background and Issues for Congress' (Congressional Research Service, 14 August 2024), https://crsreports.congress.gov/product/details?prodcode=R45811.

37 Paul van Hooft, Lotje Boswinkel, and Tim Sweijs, 'Shifting Sands of Strategic Stability: Towards a New Arms Control Agenda', 2022, https://hcss.nl/report/arms-control-shifting-sands-of-strategic-stability/.

38 Dean Wilkening, 'Hypersonic Weapons and Strategic Stability', *Survival* 61, no. 5 (2019): 129–48.; van Hooft, Boswinkel, and Sweijs, 'Shifting Sands of Strategic Stability: Towards a New Arms Control Agenda'.

39 Alan Cummings, 'Crisis Stability, OODA Loops, and Hypersonic Weapons', On the Horizon (Center for Strategic and International Studies (CSIS), 2021), https://www.jstor.org/stable/resrep29483.6.

40 Syed Sadam Hussain Shah, 'The Perils of AI for Nuclear Deterrence', *CISS Insight Journal* 7, no. 2 (2019): 6.

41 Jeffrey Hill, "Hypersonic Highly-Maneuverable Weapons and Their Effect on the Deterrence Status Quo," in *Assessing the Influence of Hypersonic Weapons on Deterrence*, by Paige P. Cone, The Counterproliferation Papers, Future Warfare Series No. 59, June 2019, 68.

missile launch, missile defence, and command and control systems. One of the primary advocated benefits, and major fears, is that such an attack could be prepared for and executed almost entirely covertly.[42]

Evidence of cyberattack capabilities that could target an adversary's nuclear arsenal became clear in 2016 as "North Korea's missiles started falling out of the sky."[43] A large-scale effort to counter North Korea's missile development had begun several years earlier within the U.S. intelligence community, and it was seemingly paying off. It appears to have been a complex effort of infiltrating the missile development supply-chain to sabotage components, possibly interfering electronically with command-and-control systems, and some inclusion of electronic warfare capabilities based in South Korea. This effort constituted what is referred to as a left-of-launch approach, meaning targeting missiles before they can leave the ground, in its non-kinetic form.[44] Similar attacks conducted by Israel are also known to have occurred against Syrian air defence systems and possibly Iranian ballistic missile launch sites, likely with US assistance. A brief list of likely cyber-sabotage and espionage attempts against nuclear sites is found below:[45]

- **2005 Operation Titan Rain -** hackers supposedly linked to China infiltrated US military systems looking for nuclear secrets.[46]
- **2006 -** Trojan planted in the run-up to Operation Orchard (2007) – Israeli Mossad planted Trojan in computer of a senior Syrian government official à revealed details around the Syrian nuclear weapons programme.[47]
- **2007 Stuxnet -** A highly sophisticated computer worm, it is believed to have been a joint operation by the U.S. and Israel, designed to sabotage Iran's nuclear enrichment facilities by causing physical damage to centrifuges through exploiting zero-day vulnerabilities.[48]
- **2011 the Zeus** malware – information-stealing Trojan which also targeted British contractors involved in building UK Trident nuclear-armed submarine force.[49]
- **August 2022** – "Hackers targeted the website of Ukraine's state energy agency responsible for the oversight of Ukraine's nuclear power plants. The agency stated Russian hackers carried out the attack."[50]

---

42 Louk Faesen et al., 'The Cyber Arms Watch: Uncovering the Stated & Perceived Offensive Cyber Capabilities of States', Cyber Arms Watch (The Hague: The Hague Centre for Strategic Studies, 2022); David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (Brunswick, Victoria: Scribe Publications, 2018).

43 Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, 150.

44 Sanger, 150–52.

45 Andrew Futter, 'Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy', 22 May 2024, 19-20, https://rusi.orghttps://rusi.org.

46 William T. Hagestad, *21st Century Chinese Cyberwarfare: An Examination of the Chinese Cyberthreat from Fundamentals of Communist Policy Regarding Information Warfare through the Broad Range of Military, Civilian and Commercially Supported Cyberattack Threat Vectors* (Ely, Cambridgeshire, United Kingdom: IT Governance Publishing, 2012), 12.

47 Erich Follath and Holger Stark, 'The Story of "Operation Orchard": How Israel Destroyed Syria's Al Kibar Nuclear Reactor', *Der Spiegel*, 2 November 2009, sec. International, https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html; Andrew Garwood-Gowers, 'Israel's Airstrike on Syria's Al-Kibar Facility: A Test Case for the Doctrine of Pre-Emptive Self-Defence?', *Journal of Conflict & Security Law* 16, no. 2 (2011): 263–91.

48 Paul K. Kerr, John Rollins, and Catherine A. Theohary, 'The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability' (Washington, D.C.: Congressional Research Service, 9 December 2010), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-040.pdf.

49 Richard Norton-Taylor and Julian Borger, 'Chinese Cyber-Spies Penetrate Foreign Office Computers', *The Guardian*, 4 February 2011, sec. World news, https://www.theguardian.com/world/2011/feb/04/chinese-super-spies-foreign-office-computers.

50 'Significant Cyber Incidents | Strategic Technologies Program | CSIS', accessed 5 June 2024, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

- **March 2023** – South Asian hacking group executed an espionage campaign that targeted companies in China's nuclear energy industry.[51] "Researchers believe the group commonly targets the energy and government sectors of Pakistan, China, Bangladesh, and Saudi Arabia."[52]
- **August 2023** – "Suspected North Korean hackers attempted to compromise a joint U.S.-South Korean military exercise on countering nuclear threats from North Korea. Hackers launched several spear phishing email attacks at the exercise's war simulation center."[53]
- **September 2023** – Russian hackers targeted the British Ministry of Defense by stealing thousands of documents and uploading them to the dark web. "The documents contained accessibility details for a nuclear base in Scotland, high-security prisons, and other national security details. Hackers acquired the documents by breaking into a British fencing developer and gaining backdoor access to Ministry files."[54]
- **March 2024 -** Iranian hackers targeted an Israeli nuclear facility by compromising an IT network connected to it. They did not compromise the operational technology network, but leaked sensitive documents of the facility.[55]

Cyber operations run along a spectrum, ranging from lower-end efforts to breach the IT systems surrounding the wider nuclear enterprise (i.e., production facilities) and scale up to include more complex, multi-source cyber/electronic warfare attacks against an entire NC3 system and launch platforms.[56] The challenge in the more complex operations is that it often requires some type of direct human infiltration or exploitation, given how heavily guarded and air-gapped sensitive nuclear systems are. Such infiltration can take years of effort from an intelligence agency, without certainty it will pay off in the end. Despite the success of the 2016-2017 US programme against North Korea, cyber capabilities are likely to remain ancillary to kinetic attacks in any first strike, such as suppressing air defence systems.

From a deterrence stability perspective, early warning systems play a key role in maintaining the credibility of second-strike capabilities. If a cyber attack successfully disables or manipulates an adversary's early warning systems, it could severely undermine the confidence in their ability to detect and respond to an attack.[57] This could trigger a first-strike incentive for an adversary who believes that an opponent may not be able to detect or respond to an initial strike. Furthermore, the uncertainty created by the compromised early warning system may lead states to question their reliance on these technologies, potentially prompting them to expand their nuclear arsenals or develop redundant early warning networks to mitigate this risk.[58] This could result in an arms race, as each side seeks to ensure that its early warning capabilities remain functional even in the face of potential cyber threats.[59]

Crisis stability is particularly vulnerable to cyber attacks on early warning systems. During periods of heightened tension, when military actions are closely monitored, a cyber attack

---

51 Ryan Robinson, 'Phishing Campaign Targets Chinese Nuclear Energy Industry', Intezer, 24 March 2023, https://intezer.com/blog/research/phishing-campaign-targets-nuclear-energy-industry/.

52 'Significant Cyber Incidents | Strategic Technologies Program | CSIS'.

53 'Significant Cyber Incidents | Strategic Technologies Program | CSIS'.

54 'Significant Cyber Incidents | Strategic Technologies Program | CSIS'.

55 'Significant Cyber Incidents | Strategic Technologies Program | CSIS'.

56 Thomas Rid and Peter McBurney, 'Cyber-Weapons', *The RUSI Journal* 157, no. 1 (February 2012): 6–13, https://doi.org/10.1080/03071847.2012.664354.

57 van Hooft, Boswinkel, and Sweijs, 'Shifting Sands of Strategic Stability: Towards a New Arms Control Agenda'.

58 Page O. Stoutland and Samantha Pitts-Kiefer, 'Understanding the Cyber Threat to Nuclear Weapons and Related Systems', *Nuclear Threat Initiative*, 2018, 9–20.

59 van Hooft, Boswinkel, and Sweijs, 'Shifting Sands of Strategic Stability: Towards a New Arms Control Agenda'.

that disables or manipulates these systems can create confusion and miscalculation.[60] For instance, if a state believes its early warning system has detected an incoming missile attack due to a cyber manipulation, it may feel compelled to launch a pre-emptive strike, believing that its adversary is preparing for a nuclear strike.[61] Similarly, if early warning systems are disabled during a crisis, decision-makers may feel the urgency to strike pre-emptively before losing their capability to retaliate. This use-it-or-lose-it dynamic exacerbates the likelihood of unintended escalation. Cyber attacks that create false positives or false negatives in early warning systems further complicate crisis stability, as states might misinterpret routine activities as hostile actions or fail to detect a genuine attack.[62] The compressed decision-making timeline that follows a perceived attack could make it impossible to verify the legitimacy of the threat, leaving leaders with little time to de-escalate the situation or correct errors.

The manipulation or degradation of early warning systems through cyber attacks thus significantly increases the risk of escalation during crisis, as it erodes the ability of states to make rational, well-informed decisions under pressure. This heightened risk of miscalculation, combined with the potential for pre-emptive strikes, poses a serious challenge to strategic stability in the nuclear age.

3.1.3. The space domain

Space-based targeting, particularly using satellite swarms (or constellations), is developing in ways that work to mitigate the intelligence problems in a possible first strike. Satellite swarms enabled with algorithms trained to support autonomous navigation and collision avoidance, dubbed "equilibrium shaping" can allow swarms of smaller, low-earth orbit (LEO) satellites to cluster over a target area more quickly to track ground movement.[63] Distributed sensing across a swarm that can manoeuvre and track targets once detected, especially more than one, would be a vital system for identifying and tracking road-mobile missile systems that are stored in underground or camouflaged positions. The disarming logic of the damage limiting first strike would rely on such targeting capability in order to acquire targets beyond airbases and pre-targeted ICBM fields.[64]

Additionally, space-based assets can support a first strike by successfully identifying which satellites form a part of an adversary's early warning network. Coupling AI-applications to space platforms, new capabilities being explored between industry and the US Defense Advanced Research Projects Agency (DARPA), called *Agatha*, claims to identify small differences in satellite behaviour to filter out commercial satellites from early-warning and intelligence ones. By analysing differences in manoeuvres and identifying deviant payloads, *Agatha* would then enable the US Space Force to accurately and precisely target adversary satellites.[65] Doing so against enemy military communications, intelligence, and possibly early-warning satellites would enable the first minutes of a first strike to be less detectable and confuse decision-makers.

---

60 Guy-Philippe Goldstein, 'Cyber Weapons and International Stability: New Destabilization Threats Require New Security Doctrines', *Military and Strategic Affairs* 5, no. 2 (2013): 121–39.; van Hooft, Boswinkel, and Sweijs, 'Shifting Sands of Strategic Stability: Towards a New Arms Control Agenda'.

61 Stoutland and Pitts-Kiefer, 'Understanding the Cyber Threat to Nuclear Weapons and Related Systems'. 2018.

62 Stoutland and Pitts-Kiefer.

63 Lorenzo Pettazzi et al., 'Electrostatic Force for Swarm Navigation and Reconfiguration', *Acta Futura* 4 (1 January 2008): 80–86.

64 Adam Koenig et al., 'ARTMS: Enabling Autonomous Distributed Angles-Only Orbit Estimation for Spacecraft Swarms', 2021, 4282–89, https://doi.org/10.23919/ACC50511.2021.9483242.

65 Snyder, para 7-8.

This of course has a direct impact on strategic stability, as even a latent capability to interfere with early-warning networks and intelligence collection could spark fears of an impending first strike. More broadly, space-based operations can significantly impact stability if used kinetically, as part of a first strike attack or otherwise. Whether a space-based electromagnetic pulse (EMP) weapon[66] or a direct-ascent anti-satellite (ASAT) attack, either would cause significant destruction. An EMP would cause mass disruption of electronics over the target area, possibly over the majority of a national territory, and an ASAT attack could create orbital debris so widespread it effectively denies space access to all who would use it. The risks and fears of space-based strikes will surely drive deep concerns and a race to find counter-solutions.

One of the most profound applications of ASAT weapons is their ability to target and destroy space-based early warning systems, which are crucial for detecting missile launches and other military activities.[67] These systems are central to deterrence stability, as they provide real-time data to detect and assess incoming threats, thus making sure that a second-strike capability is always maintained. When ASATs target these satellites, they create a significant vulnerability in an adversary's ability to detect a nuclear or conventional attack, undermining deterrence stability. The compromised ability to detect an incoming strike may prompt a pre-emptive first strike, as adversaries fear the loss of the ability to respond.

There is little reason to perceive disruption of early-warning systems as anything other than a sign of an impending first strike.

This peacetime fear is compounded in crisis scenarios, and the loss of critical surveillance infrastructure could lead to miscalculation and unintentional escalation.[68] There is little reason to perceive disruption of early-warning systems as anything other than a sign of an impending first strike. Additionally, early-warning systems are essential not only for strategic missile detection but also for the management of conventional military forces, meaning the effects of ASAT use can spill over into non-nuclear domains and civil domains, further amplifying their destabilizing potential. [69]

3.1.4. **Directed energy weapons**

Directed energy weapons (DEW) are one of the more novel developments in modern conflict. Various types and applications are at different stages of maturity. High-energy lasers, while precise and fielded in some missile defence missions, are affected by atmospheric conditions, while high power microwave emitters are not and can have larger impact over a wider area. At the highest, most experimental end, particle beam weapons have high speed, high ability to penetrate materials (such as a missile fuselage or satellite skin), and can operate in all weather conditions. However, given the energy requirements and the size of units, these systems are too complex for combat use at the time of writing.[70]

66 Michael Williams Liptak Kevin, 'White House Confirms US Has Intelligence on Russian Anti-Satellite Capability | CNN Politics', CNN, 15 February 2024, https://www.cnn.com/2024/02/15/politics/white-house-russia-anti-satellite/index.html.

67 Christopher F. Chyba, 'New Technologies & Strategic Stability', *Daedalus* 149, no. 2 (1 April 2020): 150–70, https://doi.org/10.1162/daed_a_01795.

68 Chyba.

69 Clementine G. Starling-Daniels and Mark J. Massa, 'Russian Nuclear Anti-Satellite Weapons Would Require a Firm US Response, Not Hysteria', *Atlantic Council*, 15 February 2024, https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-nuclear-anti-satellite-weapons-would-require-a-firm-us-response-not-hysteria/.

70 Mike Culhane and Jacynthe Touchette, 'Directed Energy Weapons' (Innovation, Science and Economic Development Canada, 12 February 2024), https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/emerging-technology-trend-cards/directed-energy-weapons.

When it comes to fears of a first strike, it is not immediately clear how DEWs will impact strategy stability. It is possible that DEW attacks on space assets could help to facilitate a first strike, and a race to develop such a system could precipitate fears of a future first strike. Given that much of the technology is nascent and often relies on line-of-sight and atmospheric conditions, it is not presently possible to make any definitive assessment of DEWs' strategic stability impact. Indeed, as highlighted in the survey data above, international nuclear experts do not rank DEW highly in its current stability impact. Their possible missile defence applications, and how this may affect stability, is discussed in chapter five below.

3.1.5. **Artificial intelligence**

There are a variety of artificial intelligence applications which could facilitate improved first strike capabilities. Improved autonomy in target detection and in-flight modifications to missile trajectories can improve the performance of first strike systems to accurately launch a bolt from the blue salvo against an adversary's nuclear arsenal. When coupled with a damage limitation strategy, AI applications in the wider intelligence apparatus can directly impact strategic stability by influencing the assessments of decision-makers about the possible need or feasibility of launching an attempted disarming attack. AI on mobile platforms like drones could help process data in real time and alert commanders of potentially suspicious or threatening situations such as military drills and suspicious troop or missile launcher movements.[71] There will then be the question of how well the algorithms on which the systems are based have been trained, and if they take adequate account of differences in military approaches between adversaries. What constitutes a genuine indicator in one case, say Russia, is not the same as in China or North Korea.

AI-augmented ISR systems and advances in remote sensing technologies—such as space-based radars, infrared sensors, and persistent monitoring systems—are rapidly transforming strategic stability. The impact on deterrence stability is significant, as deterrence relies heavily on states' ability to maintain secure second-strike forces, ensuring they can retaliate even after absorbing a first strike.[72] The stealth and survivability of platforms like strategic nuclear submarines (SSBNs) are central to this. However, AI-enhanced ISR systems could threaten this by creating radical transparency in military environments.[73] With these advanced technologies, adversaries can track the movements of nuclear submarines, mobile missile launchers, and other previously hard-to-detect platforms in real-time.[74] This undermines confidence in the survivability of these critical nuclear assets, weakening the credibility of second-strike capabilities.

As a result, states may feel increasingly vulnerable to pre-emptive strikes, particularly if they believe their nuclear forces can be tracked and neutralized before they can retaliate. This dynamic shift the strategic balance toward first-strike incentives. The effects on crisis stability are equally concerning. If states believe their nuclear platforms—such as SSBNs—are being tracked and could soon be neutralized in a crisis situation, they may feel pressured to launch a

71 Sarah Scoles, 'When Deepfakes Go Nuclear', *Coda Story* (blog), 28 November 2023, https://www.codastory.com/authoritarian-tech/ai-nuclear-war/.

72 Johnson, James S. "Artificial Intelligence: A Threat to Strategic Stability." *Strategic Studies Quarterly* 14, no. 1 (2020): 16–39.

73 Johnson, James. "Artificial Intelligence in Nuclear Warfare: A Perfect Storm of Instability?" *The Washington Quarterly* 43, no. 2 (April 2, 2020): 197–211. https://doi.org/10.1080/0163660X.2020.1770968.

74 Chyba, Christopher F. "New Technologies & Strategic Stability." *Daedalus* 149, no. 2 (April 1, 2020): 150–70. https://doi.org/10.1162/daed_a_01795.

pre-emptive strike before losing their ability to retaliate. This pressure to act quickly, coupled with the fear of being targeted in real-time, raises the risk of unintended escalation.

Beyond these immediate applications, experts argue that the real impact of AI on strategic stability lies less in the actual efficacy of its applications, but rather in the uncertainty it is feeding.[75] Mutual fears of losing control of escalation, of possible first strikes, and the erosion of missile defences is already fuelling a cycle of distrust. Plausible scenarios are emerging in which fears of an enemy silver bullet could cause a miscalculation and attendant "use it or lose it" view amongst civilian and military officials and cause inadvertent escalation in a crisis.[76] A particularly concerning aspect of these fears are the lack of empiricism, especially amongst US policymakers. When asked in several Chatham house sessions, senior US officials involved both in defence affairs and export control policy development (to limit Chinese military applications of AI) could not name a specific programme or system that the Chinese armed forces were developing or fielding which was feeding concerns about stability. This then opens questions of where such fears of an "AI arms race" come from. Michael Brenes and William Hartung have convincingly argued that there is a connection between threat inflation related to artificial intelligence and the Silicon Valley community that is trying to develop AI-enabled capabilities for the US Department of Defense.[77] This could well be the case, and is a phenomenon well studied in the past by nuclear scholars.[78]

3.2. **Survey findings**

Approximately two-thirds of the experts surveyed indicated hypersonic weapons (68%) and space capabilities (62%) as having a significant impact on strategic stability, particularly on first strike/counterforce tasks (68% and 62% respectively). Meanwhile, approximately half of the respondents also highlighted their relevance for "Bolt from the Blue" tasks, with hypersonic weapons gathering slightly higher agreement (56%) compared to space capabilities (47%).

The results on hypersonic weapons should not come as a surprise given their speed, manoeuvrability and ability to evade missile defences. These features compress early-warning timelines and undermine confidence in second-strike survivability, thereby exacerbating first-strike instability and significantly impacting on both deterrence and crisis stability. Similarly, the capacity of space capabilities to enhance targeting by identifying concealed counterforce or counterstrike assets, and to interfere with early-warning and intelligence systems, can greatly affect strategic stability, by decreasing the confidence in retaliatory capabilities once absorbed a first-strike.

In contrast, the survey results highlight that the effects of cyber, directed energy, and AI technologies on offensive tasks were perceived by the majority of the experts to be more limited. For first strike/counterforce tasks, cyber and AI were each rated as greatly impactful by only

75 Edward Geist and Andrew J Lohn, 'How Might Artificial Intelligence Affect the Risk of Nuclear War?', 2018, 15.

76 James Johnson, 'Artificial Intelligence & Future Warfare: Implications for International Security', *Defense & Security Analysis* 35, no. 2 (3 April 2019): 152, https://doi.org/10.1080/14751798.2019.1600800.

77 Michael Brenes and William D. Hartung, 'Private Finance and the Quest to Remake Modern Warfare' (Washington, D.C.: Quincy Institute for Responsible Statecraft, 3 June 2024), https://quincyinst.org/research/private-finance-and-the-quest-to-remake-modern-warfare/.

78 Charles L. Glaser, 'The Causes and Consequences of Arms Races', *Annual Review of Political Science* 3, no. Volume 3, 2000 (1 June 2000): 251–76, https://doi.org/10.1146/annurev.polisci.3.1.251.

24% of the respondents, while directed-energy technologies were rated by only 14% of the expert to be a key concern. Similarly, for "Bolt from the Blue", cyber and AI were deemed impactful by 14% and 19% of the experts, with directed-energy receiving the lowest rating at just 9%.

These results are perhaps also not entirely surprising: these EDTs are mostly seen as auxiliary to kinetic attacks that ultimately are required for an effective first-strike. Cyber operations, for instance, are auxiliary rather than standalone capabilities. Directed-energy weapons remain in their developmental stages, with technological and operational challenges — such as power requirements and range limitations — hindering their application to large-scale-kinetic offensive operations. Similarly, AI, though transformative in intelligence, surveillance, and decision-making, primarily enhances existing functions rather than – as of yet at least – changing the offense-defence balance dramatically in favour of the offensive. These technologies are more often associated, as the survey results show, with C3 Disruption and more-limitedly to defence tasks.

Strategic Task		Hypersonic	Cyber	Directed-Energy	Space Capabilities	AI
Offence	First Strike/Counterforce	68%	24%	14%	62%	24%

4. Interfering with command and control through deception, disruption, and confusion

Disrupting NC3 mechanisms and systems is destabilising whether a part of a first strike attack or not. This is principally because the deliberate interference in such systems will likely create the impression that the interference is part of an incoming attack.[79] Many of the areas above impact stability by default, as an attack by an HGV-enabled missile, by a satellite, or from a directed-energy weapon on an NC3 asset would almost certainly be interpreted as part of an attempted disarming first strike. This section then will focus specifically on the impact of cyberweapons and artificial intelligence on strategic stability as it relates to NC3 interference.

The disruption of NC3 ranges across a spectrum of activities, with the lowest end including deception measures such as data manipulation and fakes and the highest end including direct cyberattacks and provocative deepfakes during a crisis. Taking this entire spectrum into account, the below developments in cyber warfare and artificial intelligence bode ill for stable relations between those seeking to advance these systems.

4.1. Cyberweapons

A report by the Stanley Center for Peace and Security argues that "cyberattack methods such as data manipulation, digital jamming and cyber spoofing could jeopardize the integrity of communication, leading to increased uncertainty in decision-making...with potentially devastating consequences."[80] Particularly in a crisis, clear communications across a variety of actors is vital. Within a single state, it is imperative political decision-makers can be in near-constant communication with military officials and even operational units with nuclear warheads if necessary. Secondarily, being able to communicate intentions to an adversary

79 Paul van Hooft, Davis Ellison, and Tim Sweijs, 'Pathways to Disaster: Russia's War against Ukraine and the Risks of Inadvertent Nuclear Escalation', Strategic Stability: Deterrence and Arm Control (The Hague: The Hague Centre for Strategic Studies, May 2023), https://hcss.nl/report/pathways-to-disaster-russias-war-against-ukraine-and-the-risks-of-inadvertent-nuclear-escalation/.

80 Beyza Unal and Patricia Lewis, 'Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities, and Consequences', Stanley Center for Peace and Security, 6 September 2019, 4, https://stanleycenter.org/publications/cybersecurity-of-nuclear-weapons-systems-threats-vulnerabilities-and-consequences/.

and allies can be crucial in managing escalation and perceptions of activities. Certain cyber-weapons aim to disrupt those exact channels of communication in order to sow doubt and deception in the event of an attack, risking the erosion not only of wider stability, but of escalation in the event of conflict.

A challenge in making a clear assessment on the newly emerging challenges in cybersecurity is that the cyber domain is itself evolving constantly. It is also a misnomer to refer to a cyber-weapon as such. What is more accurate is to consider the risks stemming from zero-day vulnerabilities, or essentially software or hardware bugs of which the vendor (e.g. Microsoft) is unaware and there is no available patch. Exploits, or delivery mechanisms, are tools (code) that take advantage of such vulnerabilities and can range in effects from a distributed denial of service (DDos) attack that disrupts an unclassified network, to the more valuable vulnerabilities that allow an infiltrator to run their own code on a system. These vulnerabilities are sometimes known to intelligence services and are not communicated to vendors, as those same agencies may want to exploit the vulnerabilities in the future. Such was the case with the EternalBlue exploit software developed by the US National Security Agency to take advantage of a vulnerability in Microsoft that allowed a user to access computers across the network.[81] The risks of such vulnerabilities in NC3 systems is raised repeatedly in the 2022 US Nuclear Posture Review, and had been raised previously as well.[82] Zero-day vulnerabilities, given that they cannot be patched in advance because they have not been identified, are raised specifically as giving an adversary a perceived first mover advantage in a possible crisis.

Action in cyberspace intended to prevent nuclear escalation could unintentionally bring it about.

What exacerbates the existing challenge is the increasing use of automated cybersecurity software to counter the near constant attempts to breach classified and other sensitive systems. It is quite possible in the near future that algorithmic changes can be made autonomously and at machine speed, in milliseconds. AI-enabled cyber weapons would not have to rely on human operators to guide an attack and, if necessary, to rewrite software code to exploit newly found vulnerabilities, thus ensuring that less mistakes would be made.[83] Automated cyber defence could lead to a counterattack against a target that is perceived as deeply risky to an adversary, such as a command-and-control system. Naturally, programmers can avoid such risks with prescribed rules for defensive software, however, should one or more states begin to automate responses in irresponsible ways, this could negate the steps other states take.

Action in cyberspace intended to prevent nuclear escalation could unintentionally bring it about. The threat and fear of possible cyber vulnerabilities about the safety and reliability of nuclear forces can trigger higher states of alert in an opponent. High alert states, anxiety, and unclear information between systems is a situation ripe for accidents, errors, and ultimately tragic miscalculation.[84] Former White House cybersecurity adviser Richard Clarke has also warned that, "So, what if someone were able to hack their way into the U.S. nuclear command and control system? Let's say they wanted to start a war between Russia and the United States. Theoretically, they could trigger a false alarm, making us think that Russian nuclear weapons were on their way. Under current U.S. protocols, the president has just minutes to decide whether or not to launch a retaliatory strike and thereby, start a full-blown nuclear war."[85] Automated systems, false alarms, and zero-day vulnerabilities are continual risk to stability.

81 Nadav Grossman, 'EternalBlue - Everything There Is To Know', Check Point Research, 29 September 2017, https://research.checkpoint.com/2017/eternalblue-everything-know/.

82 '2022 Nuclear Posture Review' (Washington, D.C.: US Department of Defense, October 2022), https://s3.amazonaws.com/uploads.fas.org/2022/10/27113658/2022-Nuclear-Posture-Review.pdf.

83 Benjamin Rhode, 'Artificial Intelligence and Offensive Cyber Weapons', *Strategic Comments* 25, no. 10 (26 November 2019): x–xii, https://doi.org/10.1080/13567888.2019.1708069.

84 Ariel E Levite et al., 'China-U.S. Cyber-Nuclear C3 Stability', 2019, 19.

85 *Breaking Down the Cyber-Nuclear Threat*, 2022, 2:11-2:37, https://www.youtube.com/watch?v=A1R2ljrha4U.

4.2. **The space domain**

A critical application of ASATs is their potential use in decapitation strikes aimed at disabling an adversary's NC3.[86] By targeting satellites that form part of these networks, ASATs can significantly degrade or even sever the link between national leadership and their nuclear forces, potentially preventing a retaliatory strike. The implications for crisis stability are significant. During a conflict, states might not be able to distinguish whether the destruction of ISR satellites is part of the conventional phase of warfare or a prelude to a nuclear strike.[87] This ambiguity blurs the line between conventional and nuclear warfighting, increasing the risks of unintended escalation. Additionally, the loss of critical space-based capabilities could force states to adopt more aggressive postures, potentially rushing to escalate before their military position becomes untenable.

Non-kinetic ASATs, such as lasers and electromagnetic pulse (EMP) weapons, disrupt satellites without physical destruction, making attribution more difficult. [88] These non-kinetic methods pose their own challenges to crisis stability by causing temporary or reversible damage to space-based assets, making it difficult to assess the severity of an attack. States might overreact to non-kinetic ASAT use, escalating a situation that could have otherwise remained contained.

4.3. **Artificial intelligence**

Beyond automated cyber defence, AI could have wider impacts on strategic stability by broadly "poisoning" the data upon which decision-making is based. Knowing that an adversary utilises automated analysis tools allows a state to develop countermeasures to fool such a system, thereby polluting the information upon which vital command and control functions are based. Relatedly, AI "hallucination" could lead to catastrophic circumstances if warning systems falsely believe an attack is incoming and analysts are too quick to accede to that conclusion. Beginning first with data poisoning, we show here how such manipulation can undermine strategic stability and even a shared sense of understanding between powers of their relative capabilities, risking arms race instability as well.

Poisoning an AI system can take three primary forms. First, through dataset poisoning in which incorrect or mislabelled data is introduced into a dataset. If a state is using Deep Neural Networks (DNN), these models can be disrupted if an adversary can artificially introduce small changes leading to misclassifications, the datasets upon which the DNN is trained will be out of step with reality. If the application of the DNN is to say, rapidly identify the movement and launch of a road-mobile ICBM, the risks become apparent. The second possibility is through poisoning an algorithm behind a system, by taking advantage of vulnerabilities on personal devices to disrupt the final model which draws on the testing data conducted on the individual device. The final result is then not the combination of actual data, but rather includes

86 Matthew Mowthorpe, The Militarization and Weaponization of Space (Lexington Books, 2004), 110; Kurt Gottfried and Richard Ned Lebow, "Anti-Satellite Weapons: Weighing the Risks," Daedalus 114, no. 2 (1985): 147–70, https://www.jstor.org/stable/20024983

87 James M. Acton, 'Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War', *International Security* 43, no. 1 (1 August 2018): 56–99, https://doi.org/10.1162/isec_a_00320.

88 Todd Harrison et al., 'Space Threat Assessment 2020', *Centre for Strategic & International Studies (CSIS)*, 30 March 2020, 2–7.

manipulations inserted upstream. Third, at the highest end, an entire model can be poisoned by hacking into a system and replacing the entire model with one's own.[89] This of course requires the type of complex cyber attacks discussed in previous sections.

Deception can be more direct as well, such as deep-faking geography to manipulate imagery intelligence (IMINT) or using AI-enabled spoofing to create fake or misleading signals can give the impression that one's capabilities are either greater or weaker than they seem.[90] Should analysis tools trend towards greater automation, as publicly available information seems to show, then bad actors could fool these tools by creating false impressions of troop movements, weapons readiness, and possibly fake the preparations for a nuclear launch. Additionally, AI systems if poorly trained or interfered with, could hallucinate false impressions anyway and give analysts false alarms of impending attacks.[91] The NATO Science and Technology Organisation has already flagged such deception possibilities, noting cases wherein tanks could be misread as cars, tents were not identified at all, and basic camouflage was able to deceive even more advanced infrared sensing. [92]

Command and control systems, particularly those that support nuclear decision-making, are increasingly vulnerable to cyberattacks and manipulation in automated analysis systems. Such automated systems are increasingly being explored. One example is an experimental US Air Force capability, named "Rainfly", which aims to use "novel artificial intelligence-enabled methodologies to discover and characterize adversaries' defense systems to gain insight into organizational functionality."[93] Should such a system come to inform US Air Force decision-makers regarding how an enemy's organisation functions, this could pose risks to stability if that information is flawed or has been manipulated with in some way. Such projects merit close scrutiny and transparency.

4.4. **Survey findings**

The survey results reveal a substantial consensus regarding the disruptive potential of space capabilities (81%) and AI (66%) on command, control, and communication (C3) systems through targeting and analysis tasks. These technologies were followed by cyber weapons, rated impactful by 52% of respondents. In contrast, hypersonic weapons (16%) and directed-energy weapons (5%) were deemed by a much smaller number of experts to affect these tasks.

The emphasis remained on cyber capabilities and AI also in deception measures tasks, with more than half (52% each) of the respondents identifying their greatly disruptive potential. Space capabilities, while slightly less emphasised in this category, were nonetheless deemed relevant by 38% of respondents. By contrast, directed-energy and hypersonic technologies,

89 Marcus Comiter, 'Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It', Harvard Belfer Center for Science and International Affairs, accessed 29 March 2024, https://www.belfercenter.org/publication/AttackingAI.

90 Scoles, 'When Deepfakes Go Nuclear'.

91 Michael Klare, 'The Military Dangers of AI Are Not Hallucinations - FPIF', Foreign Policy In Focus, 14 July 2023, https://fpif.org/the-military-dangers-of-ai-are-not-hallucinations/.

92 'STO-Activities -', accessed 4 June 2024, https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=17369.

93 'Department of Defense Fiscal Year 2025 Budget Estimates - Air Force, Justification Book Volume 1 of 4 - Research, Development, Test and Evaluation' (US Air Force, March 2024), 101, https://www.saffm.hq.af.mil/LinkClick.aspx?fileticket=D266mM0zhFg%3D&portalid=84.

at 19% and 4% respectively, were viewed by a much smaller set of experts to affect strategic stability through this pathway, reflecting their primary focus on physical rather than informational disruption.

Concerning communication disrupting tasks, space capabilities (85%) and cyber weapons (81%) were deemed most impactful by the vast majority of the experts. AI also garnered notable attention, with 42% of experts acknowledging its disruptive potential. On the other side, hypersonic and directed-energy weapons were again perceived to be impactful by a smaller group of experts, with ratings of 24% and 38%, respectively, highlighting their comparatively narrower applicability in the C3 domain.

In summary, the survey results paint a clear picture of the growing importance of space capabilities, cyber tools, and AI in undermining C3 systems. Space-based systems can target satellites and communication nodes, disrupting early-warning systems and sowing uncertainty in command-and-control processes. Even unintentional interference with NC3 mechanisms can be misinterpreted as a precursor to a first-strike, heightening first-strike instability and the risk of catastrophic escalation. Similarly, space technologies, compromising intelligence-gathering systems and disrupting secure communication networks, space technologies contribute to the broader destabilising potential identified by respondents.

In the same fashion, AI-enabled systems further compound these risks by enabling advanced deception techniques, including data poisoning, deepfake imagery, and algorithmic manipulation. These technologies can effectively "poison" decision-making processes by introducing false information into automated analysis systems. For example, AI hallucinations or the deliberate insertion of misleading signals can create the illusion of imminent threats, prompting hasty or erroneous responses. Such dynamics are increasingly concerning as C3 systems rely more on AI for operational analysis and intelligence.

Cyberweapons, too, stand out as a critical threat in the disruption of NC3 systems. Their ability to create confusion and sever essential communication links at pivotal moments presents a unique and destabilizing challenge. Tools like zero-day vulnerabilities, data manipulation, and digital jamming can compromise both the content and reliability of transmitted information, heightening uncertainty during crises. The literature repeatedly warns of the escalation risks associated with cyberattacks, especially those targeting sensitive NC3 systems. Moreover, the integration of AI into cyber weapons amplifies these risks, as AI-enabled tools can autonomously exploit vulnerabilities at machine speed, leaving little room for human intervention to de-escalate tensions.

In contrast, the limited perceived impact of hypersonic and directed-energy weapons on C3 disruption is consistent with their primary focus on kinetic effects rather than electronic or informational warfare. While these technologies might play complementary roles, such as targeting physical C3 infrastructure, their contribution to the broader spectrum of disruption appears limited in comparison to cyber, artificial intelligence, and space capabilities.

Strategic Tasks		Hypersonic	Cyber	Directed-Energy	Space Capabilities	AI
C3 Disruption	Targeting and Analysis	16%	52%	5%	81%	66%
	Deception Measures	4%	52%	19%	38%	52%
	Disrupting Communications	24%	81%	38%	85%	42%

5. Protecting, concealing, and delegating: Defending the ability to conduct a second strike

As discussed in chapter two, attempts to achieve a disarming first strike will always spur a response in developing defensive capabilities. Building a secure second-strike capability, one that can withstand an initial attack and thereby assure the ability to retaliate, is the bottom-line for nuclear armed states. This requirement is what led to the development of SSBNs, road-mobile missile launchers, and is the logic behind maintaining a triad of air-, sea-, and land-delivered weapons. A major element incorporated into second strike security is the ability to defend against a first strike, the focus of this section. Improved defences, while seemingly benign, are often perceived as a capability related to the ability to conduct a first strike while limiting exposure to retaliation. Such is the logic of defensive systems reducing stability rather than supporting it.

Improvements in missile defence, cybersecurity, space-based systems, directed energy weapons, and artificial intelligence can all play a role in preserving a state's second strike. Some are combined, such as hypersonic missile defence, directed energy weapons, and satellite swarms and are treated as such here. Defensive cyber activities and the risks which can lead to inadvertent escalation, have been explored in greater detail above. Artificial intelligence is explored in greater detail, given the broader impact it can have on second strike assessments. Each combination is explored in turn and is assessed in its relationship to wider stability considerations.

5.1. Hypersonic systems, directed energy weapons, satellite swarms and missile defence

Leveraging developments in hypersonic and DEW technology for missile defence are some of the leading efforts amongst major states' military research and development areas. The US Missile Defence Agency and the European Defence Agency each are exploring the

possibilities of developing hypersonic interceptor missiles to counter incoming hypersonic attacks.[94] Increasingly, DEW systems have also been included in these R&D efforts, with states including the U.S., Israel, and South Korea already fielding these systems to target lower-speed threats such as drones and even some missiles.[95] There are, however, technological and even structural hurdles that remain in fully implementing such defensive systems in the field, particularly for the higher-order defence missions against incoming ballistic and HGV threats.

There are ongoing debates about how feasible defence against HGVs is. Some, including experts at the Dutch TNO research institute, argue that tracking such threats is becoming more possible and that irregular waveforms combined with advanced signal processing "can significantly increase the detection performance and the measurement accuracy [of hypersonic threats] compared to multiple, medium pulse repetition frequency waveforms with linear signal processing".[96] This development, which moves beyond the existing systems for ballistic missile defence, is reportedly also under consideration at DARPA in the US. Others argue that "hypersonic missiles can be detected by existing space-based sensor technologies" and that "given the predicted spatial precision of the SBIRS system and its short revisit time, tracking hypersonic gliders through most of their flight is likely feasible."[97] Relatedly, defence industry representatives in the US (from Raytheon and Northrop Grumman) claim their experimental Glide Phase Interceptor Weapon will be effective in intercepting HGVs in their glide phase.[98] Sceptics have pushed back on these more optimistic assessments, arguing that the technology for interceptors is still far from proven and that tracking would be far more difficult in practice, especially against multiple simultaneous targets.[99] Much of this debate is reflective of existing discussions over ICBM defence, and whether such technologies risk stability or are worth their substantial costs.[100]

Direct interception relies critically on space-based sensors, an area in which satellite swarms can increasingly play a part. Swarms can enhance target detection through distributed sensing, covering larger areas with higher resolution and redundancy, which can be used to better track hypersonic and ballistic weapons. It could well be possible that despite the unique qualities of HGVs (speed and manoeuvrability), improved space-based sensing could make up for deficits in existing BMD arrangements.[101] However, Frank Peterkin from the US Office

94 Jennifer DiMascio and Kelley M. Sayler, 'Hypersonic Missile Defense: Issues for Congress' (Washington, D.C.: Congressional Research Service, 24 June 2024), https://sgp.fas.org/crs/weapons/IF11623.pdf; 'EUropean HYpersonic DEFence Interceptor Takes Off', European Commission, 31 October 2023, https://defence-industry-space.ec.europa.eu/european-hypersonic-defence-interceptor-takes-2023-10-31_en.

95 Hyung-Jin Kim, 'South Korea to Deploy Laser Weapons to Intercept North Korean Drones', AP News, 11 July 2024, https://apnews.com/article/south-korea-laser-weapons-north-drones-4220fd7713dc5e42351fede6f56ebe11; 'What Is Israel's Iron Beam?', The Economist, 13 November 2023, https://www.economist.com/the-economist-explains/2023/11/13/what-is-israels-iron-beam; Jon Harper, 'Pentagon's Directed Energy Guru Sees "Uncomfortable Choices" Ahead for Military Commanders', *DefenseScoop* (blog), 23 January 2024, https://defensescoop.com/2024/01/23/directed-energy-weapon-pentagon-peterkin-uncomfortable-choices/.

96 Pepijn Cox, Keith Klein, Mario Coutiño and Laura Anitori, 'Improved Detection of Hypersonic Threats with Radar Using Irregular Waveforms and Advanced Processing', European Defence Agency, tno.nl/en, 16 June 2023, https://www.tno.nl/en/newsroom/2023/06/earlier-detection-hypersonic-missiles/.

97 Cameron L. Tracy and David Wright, 'Modeling the Performance of Hypersonic Boost-Glide Missiles', *Science & Global Security* 28, no. 3 (1 September 2020): 158, https://doi.org/10.1080/08929882.2020.1864945.

98 John Keller, 'Raytheon, Northrop Grumman Move Forward on Glide Phase Intercept (GPI) Hypersonic Missile Defense Project', Military Aerospace, 20 November 2023, https://www.militaryaerospace.com/sensors/article/14301696/raytheon-technologies-corp-hypersonic-missile-defense-glide-phase-intercept-gpi.

99 G. Mashkov, 'Hypersonic Weapons: Strategic Breakthrough or Strategic Challenge?, Hypersonic Weapons: Strategic Breakthrough or Strategic Challenge?', 31 October 2023.

100 'Hypersonic Weapons and the Future of Nuclear Deterrence', p. 35.

101 Ramin Skibba, 'The Space Force Is Launching Its Own Swarm of Tiny Satellites – Space Development Agency', accessed 29 March 2024, https://www.sda.mil/the-space-force-is-launching-its-own-swarm-of-tiny-satellites/.

of the Under Secretary of Defense for Research and Engineering has noted that while the technology itself may prove to work in the future, the primary challenge is its integration into the actual defensive architecture in practice. Issues of command and control of space assets, communications with decision-makers, and the connectivity between distributed space assets and other threat assessments would need to evolve in order to ensure that if a threat does emerge, that those who are behind the operating system are able to fuse the information in enough time to generate a response.[102]

Outside of direct intercept technologies, other research has stressed the possibilities of DEW in hypersonic missile defence. In 2024, the UK Ministry of Defence published a press release on the new RFDEW (Radio Frequency Directed Energy Weapon) which is "significantly cost-effective" and could be ready as early as 2025.[103] The "system can neutralise a swarm of drones for 10p a shot", "offers operational advantage and battlefield protection" and "will be operated by [UK Armed Forces] in the coming years."[104] This system, however, is only under development to counter drone swarms, and would require significant scaling and development in order to counter an HGV. Such a nascent capability is reportedly under development by Northrop Grumman in the United States.[105]

Overconfidence in missile defence systems could impact stability by giving the false impression that a damage limitation approach would work at acceptable cost.

Should either direct interception or DEW systems become feasible for HGV defence, this would have a similar effect on strategic stability as have existing ballistic missile defence systems. By making oneself less vulnerable to strategic attack, this could lead a state to become more optimistic about a first strike being feasible while taking acceptable losses (i.e., a damage limitation strategy). Further, overconfidence in missile defence systems could impact stability by giving the false impression that a damage limitation approach would work at acceptable cost, while simultaneously dooming millions who are unprotected by faulty missile defences. This is, essentially, an old debate packaged in the language of emerging and disruptive technologies.

5.2. Artificial intelligence and "Dead Hand" delegation

By far the most destabilising use of artificial intelligence in possible strategic applications is the concept of a "dead hand" or "fail-deadly" system for nuclear use. Advocates for such a system describe it as being able to "both detect an inbound attack more rapidly than the current system and allow the president to either manually direct forces to respond or automatically execute the president's pre-selected response options."[106] Critics argue that such a system would be "inappropriate, unnecessary, and dangerous" and that there is no reason to

102 Harper, 'Pentagon's Directed Energy Guru Sees "Uncomfortable Choices" Ahead for Military Commanders'.

103 'Cut-Price Anti-Drone Weapon Could Be Ready next Year', accessed 27 June 2024, https://www.ft.com/content/3675f8ad-0a9c-45e4-9454-fc1212a1b487.

104 'Cutting-Edge Drone Killer Radio Wave Weapon Developing at Pace', GOV.UK, accessed 27 June 2024, para. 1-3, https://www.gov.uk/government/news/cutting-edge-drone-killer-radio-wave-weapon-developing-at-pace.

105 'Counter Hypersonics', Northrop Grumman, n.d., https://www.northropgrumman.com/space/counter-hypersonics.

106 Adam Lowther and Curtis McGiffin, 'America Needs a Dead Hand More than Ever', War on the Rocks, 28 March 2024, https://warontherocks.com/2024/03/america-needs-a-dead-hand-more-than-ever/.

believe such a system would actually make better or even necessarily faster decisions than a human being.[107]

But what would precisely make up such a system, and how feasible is the underlying technology? The Russian *Perimeter* system offers clues. Reportedly consisting of a command rocket and an autonomous command and control system, it functions by launching the command rocket over the length of Russian territory and sending out automated codes to ICBM siloes and launchers to fire upon receiving a signal. What remain open questions though are what fires the rocket and if the signal can be stopped once the rocket is in the air. One of the designers, Valery Yarynych, told the following to reporters in 2009, which is worth quoting in full:

> *It was designed to lie semi-dormant until switched on by a high official in a crisis. Then it would begin monitoring a network of seismic, radiation, and air pressure sensors for signs of nuclear explosions. Before launching any retaliatory strike, the system had to check off four if/then propositions: If it was turned on, then it would try to determine that a nuclear weapon had hit Soviet soil. If it seemed that one had, the system would check to see if any communication links to the war room of the Soviet General Staff remained. If they did, and if some amount of time—likely ranging from 15 minutes to an hour—passed without further indications of attack, the machine would assume officials were still living who could order the counterattack and shut down. But if the line to the General Staff went dead, then Perimeter would infer that apocalypse had arrived. It would immediately transfer launch authority to whoever was manning the system at that moment deep inside a protected bunker—bypassing layers and layers of normal command authority.*[108]

Such a fail-deadly system, then, would work through a series of automated if/then statements to determine its own ability to act. Another dead-hand, built by another state, would likely have to consider the following propositions:

1. Are there signs a nuclear attack has occurred? (Radiation, seismic activity, news alerts)
2. Are communications with command-and-control systems still operational?
3. Are there any signs of communication from political leaders?

If the first answer is yes, and the other two no, then the secret bunker mentioned by Yarynich would receive the signal to launch the command rocket.

A more advanced system using newer automated decision-making technologies (ADMT) could be technologically feasible. At the operational level, decision-support systems (DSS) have already made an appearance when it comes to targeting decisions, such as the Israeli *Gospel* and *Lavender* systems.[109] Already controversial, the systems reportedly have built-in "permissive" policies for civilian casualties, with officers having "no requirement to thoroughly check why the machine made [targeting] choices or to examine the raw intelligence data on

---

[107] Luke O'Brien, 'Whither Skynet? An American "Dead Hand" Should Remain a Dead Issue', War on the Rocks, 11 September 2019, https://warontherocks.com/2019/09/whither-skynet-an-american-dead-hand-should-remain-a-dead-issue/.

[108] Nicholas Thompson, 'Inside the Apocalyptic Soviet Doomsday Machine', *Wired Magazine*, 21 September 2009, https://web.archive.org/web/20120229031744/http:/www.wired.com/politics/security/magazine/17-10/mf_deadhand?currentPage=all.

[109] Harry Davies, Bethan McKernan, and Dan Sabbagh, '"The Gospel": How Israel Uses AI to Select Bombing Targets in Gaza', *The Guardian*, 1 December 2023, https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets.

which they were based."[110] Such an operational DSS is not manifestly different than a fail-deadly system, in that it still requires a human somewhere along the line to 'pull the trigger' based on the system's information (e.g., an officer at a command bunker). Should a fail-deadly system become normalised into training and exercising regimes, an unacceptable level of permissiveness could be engendered within the nuclear enterprise that values immediate, punishing strikes over deliberate, strategic use or restraint.

Notionally, the fear of a dead hand system could support stability if communicated clearly that any nuclear attack will receive automatic, all-out countervalue salvoes from across the triad. This is built, however, on the flawed assumption that deterrence cannot fail, and no state would be irrational enough to attack the enemy's capital. There is not a sufficiently clear reason why a dead-hand system would necessarily have more of a deterrent effect than a declared launch on warning policy. Additionally, such a system presupposes a leadership decision to respond to a decapitating attack with possibly mass countervalue attacks against entire populations. For democracies this is a particularly fraught concept as 1) it conflates the survival of the top level of government with the survival of the entire country and 2) it entirely eschews the concept of government continuity by denying a legally recognised successor the choice to end a war. A decision *not* to retaliate could easily be the case in the event of nuclear attack. Regardless, it is not for technicians in the nuclear enterprise to decide.

5.3. **Survey findings**

It is not for technicians in the nuclear enterprise to decide.

A more diversified landscape emerges with regards to the experts' assessment of the impact of EDTs on defending the ability to conduct a second strike, with notable variations across different operations. In the context of delegation of authorities tasks, AI was the single EDT to stand out, with 42% of the respondents warning for a significant impact. In comparison, space capabilities and cyber tools were each identified as impactful by only 19% of the respondents, while none of the experts (0%) ranked directed-energy and hypersonic weapons as impactful.

Where it concerned concealing assets, space capabilities were perceived as the most impactful, with 42% of the respondents highlighting their role, followed by AI at 28%, and both cyber and directed-energy weapons at 19%. Hypersonic weapons, however, were once again ranked as the least impactful EDTs among those analysed with only 4% of the experts ranking it as impactful on this task.

A slightly more homogenous picture emerged for protecting assets tasks, with almost half of the pool of respondents (47%) ranking space capabilities as highly impactful, followed by Directed-Energy at 33%, and cyber capabilities at 23%. AI and hypersonic weapons were rated as highly impactful by slightly fewer experts with 19% and 20% respectively.

Collectively, the results reveal a clear trend: for defence tasks, none of the technologies in question were rated as highly impactful by more than 50% of the respondents for any strategic task. In addition, hypersonic and cyber weapons stood out for their consistently lower impact, with neither one receiving more than 25% of respondents rating them as highly influential across any defensive task.

[110] Yuval Abraham, '"Lavender": The AI Machine Directing Israel's Bombing Spree in Gaza', *+972 Magazine*, 3 April 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/.

However, space capabilities and AI stood out as the two most-highly rated EDTs. Through distributed sensing and satellite-based networks, space capabilities enhance the concealment and protection of critical ISR assets while reducing potential vulnerabilities to a first strike. Moreover, they offer redundancy, enhancing the survivability of key components of retaliatory forcers by ensuring that operational capabilities remain functional even if some assets are compromised, while also improving the tracking of hypersonic and ballistic weapons. In addition, AI, particularly in the context of delegating authorities, is seen to significantly enhance defensive measures. AI-driven systems can support rapid decision-making, automate threat assessments, and even – although extremely dangerously – facilitate hypothetical fail-deadly systems designed to ensure retaliation in the event of decapitation. At the same, the integration of AI systems also introduces profound risks. Automation in critical C2 tasks increase the likelihood of escalation due to errors or misinterpretations. AI systems can also be subject to cyberattacks – as described earlier. The potential to destabilise rather than reinforce deterrence by ensuring retaliation depends heavily on their design and operational context, as well as the degree of communication between the actors involved regarding their use.

By contrast, roughly one-fifth of respondents considered cyber capabilities to be highly impactful on the three defensive tasks here identified. Defensive cyber operations protect sensitive networks from infiltration, ensuring the integrity of communications and safeguarding operational reactiveness. The risk of miscalculation or escalation remains high, as offensive and defensive cyber activities often blur the lines between defence and offense, and deterrence and escalation. In crisis situations involving nuclear assets, such dynamics could lead to highly destabilising consequences.

The lower ratings for hypersonic and directed-energy weapons reflect their narrower applicability and developmental challenges. Directed-energy weapons, while promising to neutralise low-speed threats like drones, face significant barriers scaling up for the protection of strategic assets against faster and more evasive incoming attacks, such as hypersonic weapons. Similarly, hypersonic weapons, while pivotal for offensive tasks, are far less developed as a defensive tool. Intercepting incoming hypersonic threats remains a major technological challenge, requiring advancements both in early detection and interception capabilities.

Strategic Tasks		Hypersonic	Cyber	Directed-Energy	Space Capabilities	AI
Defence	Delegation of Authorities	0%	19%	0%	19%	42%
	Concealing Assets	4%	19%	19%	42%	28%
	Protecting Assets	20%	23%	33%	47%	19%

6. Findings, Conclusions and Recommendations

Today, arms control advocates are exploring new ways to put the brakes on a seemingly accelerating arms race in technological developments that risk nuclear stability, as in each of the cases explored in detail above. Measure-countermeasure spirals are escalating as states pursue both first strike technologies and defensive capabilities. Further, multipolar deterrence dynamics and the possible erosion of credible extended security guarantees has only continued to place the global arms control regime under intense pressure.

In this report we have conducted a systematic analysis of the impact of EDT on strategic stability. We have focused on classic strategic stability concepts including crisis and deterrence stability and assessed how these may be affected through the impact of EDT on first strike, command and control disruption, and second strike protection. Our analysis of these pathways has been approached with caution, given how difficult it is to understand nuclear dynamics in the absence of a larger empirical evidence base. What insights can be drawn from our analysis for Sino-European engagement going forward?

A bare minimum foundation for productive dialogue is the shared recognition between European states interested in such discussions and Beijing that the EDTs above are increasingly challenging strategic stability around the world. This is seemingly the case, with a wealth of publications from European and Chinese authors on this topic highlighting the risks such technologies pose. As the summary table of our expert survey shows (see Table 2 below), there are areas of significant concern singled out by experts across the world.

Table 2. Expert Survey Result - Rate of Respondents Ranking each EDT's impact as 4 or 5 across Strategic Tasks.

Strategic Tasks		Hypersonic	Cyber	Directed-Energy	Space Capabilities	AI
Offence	First Strike/Counterforce	68%	24%	14%	62%	24%
	'Bolt from the Blue'	56%	14%	9%	47%	19%
C3 Disruption	Targeting and Analysis	16%	52%	5%	81%	66%
	Deception Measures	4%	52%	19%	38%	52%
	Disrupting Communications	24%	81%	38%	85%	42%
Defence	Delegation of Authorities	0%	19%	0%	19%	42%
	Concealing Assets	4%	19%	19%	42%	28%
	Protecting Assets	20%	23%	33%	47%	19%

Turning these shared concerns about emerging technologies and strategic stability into momentum for arms control measures is a long road. This begins with transparency. The OSCE Vienna Document provides some precedence for this in the European case with Russia, with information exchanges on military research and development programmes being a possible measure.[111] Doing so in a bilateral format between China and European states, or the EU itself for that matter, is a challenge specifically in the context of Sino-American competition and current policies of European states towards the Indo-Pacific. Yet for Europe, in the context of this competition, it is essential to engage with Beijing directly on areas of mutual concern.

As the survey has gathered, concerns about supporting technologies could create space for other discussions on EDTs. Our analysis highlights particular concern surrounding non-kinetic interference with space-based systems, especially early-warning and NC3 systems, as well as with AI and the effects it may have on strategic stability. Though it would be pushing back against the offensive strategy advocates highlighted above, pledges and meaningful verification measures to ensure such space-based systems are not interfered with are a relevant step towards improved stability. In a similar vein, abstaining from integrating AI in NC3 systems, as China and the US have agreed to, is another relevant step. The recommendations that follow below build on this.

Our analysis highlights particular concern surrounding non-kinetic interference with space-based systems, especially early-warning and NC3 systems, as well as with AI.

Our analysis yield the following five recommendations for European policymakers to consider:

1. **Build on concerns in space.** Space as a global common is at great risk in the event of war. Targeting or interfering with space-based early-warning, nuclear command and control infrastructure, or communications systems risks not only serious miscalculation and escalation, but also creating debris fields that make space less usable for all. This shared impact and concern is a platform from which dialogue can be pursued.
2. **Consider areas of unilateral restraint, in space as well as when it comes to AI-enablement.** Imposing limits on the integration of AI-applications into military systems, especially those related to decision-making involving the use of force, will be an important area to signal cooperative intent towards Beijing.
3. **Be transparent about the aims of hypersonic development.** The development and testing of hypersonic technology is fraught with opportunities for misunderstanding. From an external perspective, it communicates an aim to pursue a first strike strategy. For Europeans, this would not only be quixotic due to the size of the Russian arsenal, but also destabilising and only further arms racing tendencies. It is therefore necessary to be as transparent as possible concerning the concepts of operations and doctrines that these weapons underpin in order to reduce misperceptions.
4. **Consider closer nuclear consultation ties in Europe with France and the UK.** The existing 'iron triangle' of defence agreements between Paris, London, and Berlin (the treaties of Lancaster House, Aachen, and Trinity House) provide for a strong level of consultation on defence planning and priorities. These treaties could open the door for more frameworks outside of NATO to propose meaningful dialogue measures with other states, including China. France and the UK as Europe's independent nuclear powers gives them a vital voice in any possible arrangements.
5. **Maintain European-Chinese dialogue at the Track 1, 1.5, and 2 levels.** Dialogue with China through the upcoming Trump administration is risky given the possibility of retaliation from Washington. However, as part of establishing an independent negotiating position on EDTs, channels with Beijing should be kept open across levels, with an aim to normalising these interactions outside the narrative of Sino-American competition.

111 'Vienna Document on Confidence- and Security-Building Measures'.

What this report has established, corroborated with both international expert opinion and reviews of Chinese literature, is that there is mutual concern, perhaps concern sufficient to support momentum towards risk reduction measures and increased transparency between European states and China. The supplement to this report explores possible arms control pathways in greater detail, but understanding the impacts of these new technologies on stability underpins these arms control considerations. Rapidly pursuing and fielding EDTs that imply an attempt to achieve a disarming, first-strike advantage can only serve to accelerate spiral dynamics instead of bolstering deterrence, which is neither in Europe's interest, nor in China's.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl