



The Houthis and AI-assisted ballistic proliferation

Michel Camelot

Research Fellow, FRS

2026 | In-Depth Report

In brief

A Yemeni engineering cell, probably linked to the Houthis, used Claude to develop guided-weapons software. Anthropic identified three programmes: smartphone-based homing guidance for a guided rocket (at the testing stage), a ballistic missile with a range of at least 2,000 km (at the simulation stage), and work on a hypersonic glide vehicle (still conceptual). Together they aim at mass production, circumvention of embargoes, and penetration of missile defences. This brief argues that AI's main value lies in shortening the loop between design, testing and the next iteration, implementing the concept of 'prototype warfare'. LLM providers should therefore increase their efforts to detect misuse through aggregated behaviour, while open-weight models add additional challenges than need to be taken into account by existing missile-control regimes like the MTCR and the HCoC.

DISCLAIMER

This document was produced with financial support from the European Union. The contents of this document are the sole responsibility of the Foundation for Strategic Research and in no way reflect the position of the European Union.

Introduction

'An engineering cell based in Yemen was using Claude to develop software for guided weapons,' announced Anthropic (the company developing the large language models (LLMs),¹ Claude) in a security report entitled '*Detecting and countering misuse of AI: September 2026*'.² The unit, identified by the company under the code GTG-87001,³ used Claude to design three different programmes:

- Final-phase homing guidance software for a guided rocket intended to operate on a COTS smartphone.⁴
- A multi-stage ballistic missile with a target range of at least 2,000 km.
- A multi-variant missile, one variant of which would incorporate a Hypersonic Glide Vehicle (HGV).

Claude's operating mode was particularly well-oiled: queries were broken down as much as possible and functions separated so that safeguards⁵ could not identify the purposes associated with them and would not censor them. For example, and again according to Anthropic, some accounts carried out the searches, others asked Claude to write code, and finally, others corrected the code. This team employed what is known as 'fragmentation evasion'. After linking all the prompts together, the company had these actors' accounts closed, whilst admitting that it had evidence that they already possessed an offline simulation capability – unrelated to Claude – enabling them to continue their numerical simulations. Furthermore, although the accounts have been closed, the Yemeni actors will still be able to create new ones and, once again, attempt to circumvent the safeguards. Even if a direct link to the Houthis has not been established, it nevertheless seems reasonable to attribute this body of research to them, given that they control the region from which the research was launched and have been actively pursuing a strategy of ballistic weapons proliferation for over a decade.⁶

The question, therefore, is whether the use of an LLM by a Houthi engineering unit simply constitutes a new technical support tool, or whether it reveals a more profound transformation in the capability-building model of an actor subject to an embargo?

On the first set of queries

According to Anthropic, the guidance software running on a COTS smartphone is the most advanced programme. This software has various capabilities and incorporates several pieces of firmware, including one for flight control and another for terminal guidance. This set of capabilities fulfils the GNC (Guidance, Navigation, and Control) function. Claude's parent company does not specify the technologies to which these systems are intended to be connected.

- **Hypothesis 1:** It seems reasonable to assume that these systems could relate to electro-optical and/or infrared (EO/IR) systems. These technologies are already integrated notably into ASBMs (Anti-Ship

¹ Large Language Model: an artificial intelligence programme designed to understand, interpret and generate text in natural language.

² Anthropic, *Detecting and Countering Misuse of AI: September 2026*, p. 112.

³ GTG stands for Generative Threat Group and refers to an internal classification designating a group of actors who are misusing AI.

⁴ Commercial off-the-shelf.

⁵ Computer systems designed to prevent malicious requests from succeeding and to detect suspicious behaviour on the platform.

⁶ More precisely, since the movement seized and began modifying the Yemeni army's stockpiles.

Ballistic Missiles),⁷ of which the Houthis possess a number, most of which derived from Iranian systems. This technology could be improved or adapted here to operate on a smartphone to guide a new light ballistic missile ('guided rocket').

- **Hypothesis 2:** Another possibility would be the implementation of radar guidance technology, which has already been tried and tested on the Al-Mandeb 2 and the Sayyad, two Iranian-made ASCMs (Anti-Ship Cruise Missiles).⁸ The use of this technology could reduce errors and increase the system's reliability when EO/IR is insufficient to detect or distinguish a vessel. Improving the reliability of their systems could be a key focus of Houthi research, as many of their ASBMs crash on launch or miss their targets and fall into the sea, despite the relative immobile targets selected.⁹

As a reminder, the Houthis' most advanced ASBM systems operate using a GOLIS (Go-onto-location-in-space) system during the first phase of flight, based on inertial navigation units. When the re-entry vehicle dives towards the ground, it then employs a GOT (*Go-onto-target*) system which locates the moving target and directs the warhead towards it. Here, the report remains cautious and refers to a 'guided rocket'. It provides no further details on the vehicle's characteristics. A guided rocket is very difficult to distinguish from a ballistic missile, but traditionally, its range is generally shorter and the system's trajectory remains in the atmosphere. This type of system – and this may well have been the intended purpose – might be able to hit a target precisely. The Houthis could try to improve the accuracy of their rockets and make them more effective. For ground targets, the recognition algorithm used for terminal guidance could be trained, for instance, on the optical, infrared, or radar signatures of Saudi equipment, installations, or vehicles. It is also possible that the resulting programme was trained to strike moving targets, whether on land (less likely) or at sea (highly likely). In the case of a moving maritime target, developing a short-range delivery vehicle (a "rocket") would enable low-cost mass production. As part of an A2/AD (anti-access, area-denial) strategy applied to the Bab el-Mandeb Strait, the required range of ASBM systems is relatively limited. Indeed, it has been halved in recent days following the capture of Perim Island (located in the choke point) by the armed group.¹⁰

This series of requests is designed to develop software capable of running on a smartphone (or at least on telephone components). Like other armed groups,¹¹ the Houthis appear to be seeking to incorporate as many readily available components as possible into their weaponry. This once again highlights the intrinsic dual-use nature of electronic and digital equipment, which compensates for shortcomings in local industrialisation and difficulties with imports. The Houthis are subject to several embargoes concerning military equipment or dual-use goods. Since 2014, the European Union, through Council Regulation No 1352/2014, has prohibited 'the

⁷ Fabian Hinz, 'Houthi anti-ship missile systems: getting better all the time,' *IJSS*, 8 January 2024, <https://www.ijss.org/online-analysis/military-balance/2024/01/houthi-anti-ship-missile-systems-getting-better-all-the-time/>

⁸ *Ibid.*

⁹ See, for example, the attacks on the *Morning Tide* and the *Star Nasia*. See, 'Houthi militants fire six ballistic missiles at two ships,' *The Maritime Executive*, 6 February 2024, <https://maritime-executive.com/article/houthis-target-two-more-merchant-ships-with-new-attacks>

¹⁰ Jonathan Yerushalmy, 'Houthis seize strategic Red Sea island as analysts warn of impending oil crunch,' *The Guardian*, 15 September 2026, <https://www.theguardian.com/world/2026/sep/15/houthi-rebels-seize-red-sea-hanish-islands-saudi-oil-warning>

¹¹ Just as Hezbollah does for its domestic rocket production. See Yaakov Lappin and Tal Beerli, 'Hezbollah – Independent weapons production, a hybrid doctrine in light of a strategic need,' *Alma Research and Education Centre*, 2 November 2025, <https://israel-alma.org/hezbollah-independent-weapons-production-a-hybrid-doctrine-in-light-of-a-strategic-need/>

provision, directly or indirectly, of technical assistance related to military activities and the supply, manufacture, maintenance and use of arms and related equipment of any kind, including weapons and ammunition, military vehicles and equipment, paramilitary equipment and spare parts for the aforementioned items'.¹² The following year, the UN Security Council also adopted a resolution concerning an arms embargo on the Houthis in almost identical terms to those of the European Union.¹³ Despite the sanctions, equipment from Iran continues to pour in;¹⁴ this has constituted proven support for the rebellion since 2009.¹⁵ The desire to develop software capable of running on a smartphone reflects either a need to mass-produce missiles or a decline in imports of Iranian CNG components. In both cases, the creation of a dual-use application for civilian technology is an attempt to address a bottleneck in military technologies.

The first set of queries also illustrates the iterative process highlighted by Anthropic. The engineering team tested the prototype in real-world conditions and, in the hours that followed, analysed the causes of its failure with Claude. These rapid and varied developments – for categories of missiles already present in the arsenal (ASBMs: Asif, Tankil, Mohit, Mayun, Falaq, Al-Bahr Al-Arabi...) – seem to support the idea that drawing up a precise list of Houthi capabilities is a futile endeavour, given that this actor appears to have shifted towards what might be termed 'prototype warfare'. Lieutenant-Colonel Robert R. Leonhard (US Army) introduced this concept in *The Principles of War for the Information Age* in 1998. In his view, 21st-century wars will no longer be characterised by the use of mass-produced equipment, but by the use of a '*constant multitude of technological advances, at a pace that will not allow for mass production*'.¹⁶ Rapid iteration on a guidance system demonstrates flexibility in production, capable of quickly incorporating feedback, whether derived from experimental tests or from use for actual strikes under experimental conditions. In this case, the weapon designers shorten the engineering lead time through shorter corrective cycles. Integrating software-based assistance offers benefits, not specifically in production, but above all in design, enabling corrections drawn from previous tests to be incorporated more quickly. AI therefore does not enable instant proliferation; it does not produce a missile from start to finish. It is integrated into the development process and enhances it, but its major advantage appears to be the time saved by the producing team at the design stage. If this reading is correct, tracking specific missiles or capabilities remains necessary but is no longer sufficient. Given the number of variants likely to emerge, analysts should also monitor the pace of iteration, as the sword-and-shield dynamic is evolving in the very short term.

On the second set of queries

The Houthis are deploying and developing – notably with Iran's assistance – a range of ballistic missiles whose ranges have been steadily increasing since 2015. After seizing stocks of TBMs (Tactical Ballistic Missiles with a

¹² Council Regulation No 1352/2014 of 18 December 2014, consolidated version of 12 September 2024, Article 1a(a).

¹³ United Nations Security Council, Resolution 2216 (2015), 14 April 2015, paragraphs 14–17.

¹⁴ U.S. Central Command, 'USCENTCOM seizes Iranian advanced conventional weapons bound for the Houthis,' 16 January 2024, <https://www.centcom.mil/MEDIA/PUBLIC-RELEASES/Article/3645241/uscentcom-seizes-iranian-advanced-conventional-weapons-bound-for-houthis/>

¹⁵ Tim Michetti, *A guide to illicit Iranian weapon transfers: The Bahrain file*, Atlantic Council, Washington D.C., December 2020, p. 53.

¹⁶ Robert R. Leonhard, *The Principles of War for the Information Age*, Ballantine Books, New York, 1998, p. 72.

range inferior to 300 km¹⁷) from the Yemeni government,¹⁸ the Houthis developed local versions of the Scud-D, which reached a range of 1,000 km as early as 2017¹⁹, shifting the missiles from the SRBM (Short-range ballistic missile: 300–1,000 km) category to that of MRBM (Medium-range ballistic missile: 1,000–3,000 km). The Arabian Peninsula and Israel have been within range since 2023 with the introduction of the Toofan²⁰ and the Palestine-2.²¹

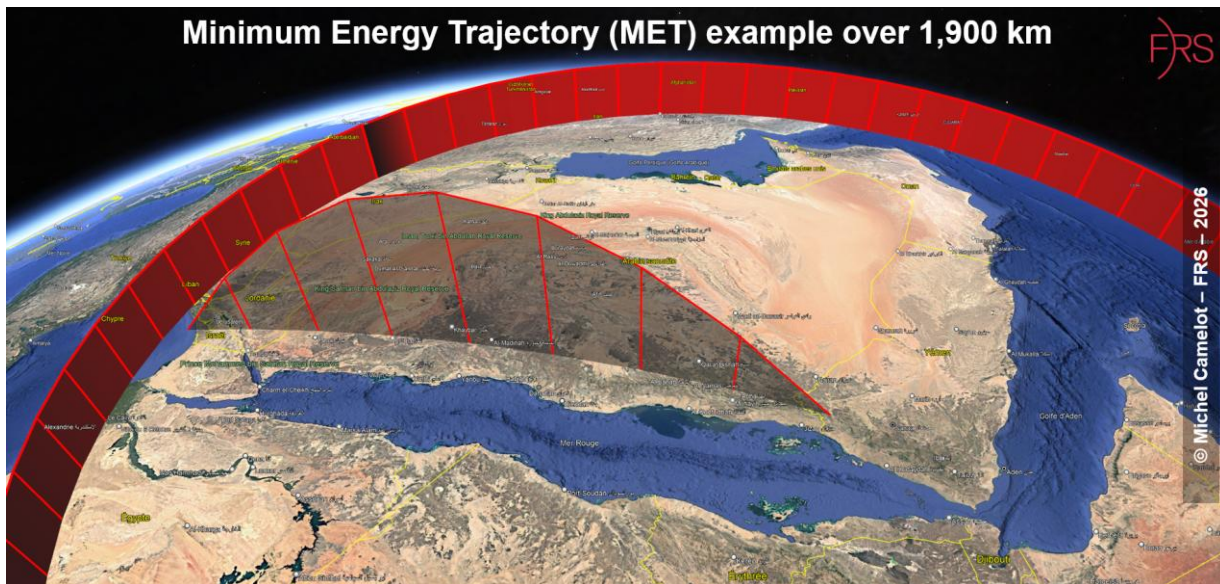


Figure 1 Illustration of a theoretical launch from Northwest Yemen against Israel, with a 2,000 km range circle drawn from the potential launch site

¹⁷ This definition is a proposal; indeed, under the MTCR, missiles with a range exceeding 300 km are subject to strict controls. For the DoD, however, a TBM is a ballistic missile with a range of less than 3,000 km.

¹⁸ Scud B or C (North Korean-manufactured Hwasong-5 or 6 exported in the 2000s), with ranges at that time ranging from 300 to 550 km. See Jean Masson, 'Les missiles des Houthis : prolifération balistique et groupes armés non-étatiques,' Research and Documents, FRS, No. 11/2018, December 2018, p. 10.

¹⁹ These include the Burkan-I, II, IIH and III, which bear a strong resemblance to certain Iranian missiles such as the Qiam-1. The Houthis claim to have developed them themselves, but Iran appears to be involved. It is unclear whether they were manufactured in Yemen or imported directly from Iran. See *ibid.*, p. 19.

²⁰ The Toofan was unveiled in 2023 and is derived from the Iranian Ghadr-S, F or H, which has a range of up to 1,950 km according to Tehran's official press. See 'Houthi Arsenal,' Wilson Centre, 26 July 2024, <https://www.wilsoncenter.org/article/houthi-arsenal>; Fabian Hinz, 'Little and large missile surprises in Sanaa and Tehran,' *IJSS*, 17 October 2023, <https://www.ijss.org/online-analysis/military-balance/2023/10/little-and-large-missile-surprises-in-sanaa-and-tehran/> and 'Which missiles did Iran use in its retaliatory attack on Israel?,' *Mehr News Agency*, 2 October 2024, <https://en.mehrnews.com/news/222300/Which-missiles-Iran-used-in-its-retaliatory-attack-on-Israel/>

²¹ A two-stage solid-propellant missile with a manoeuvrable warhead and a claimed range of over 2,000 km, possibly derived from the Khiebar Shaekan 2 unveiled in Iran in 2023. See Boaz Shapira, 'Palestine-2 missile launched by the Houthis towards Israel,' *Alma Research and Education Centre*, 18 September 2024, <https://israel-alma.org/palestine-2-missile-launched-by-the-houthis-towards-israel-september-15/>

The set of queries in this programme leads Anthropic to conclude that the group has reached the simulation stage. One may wonder why the Houthis would invest efforts in developing a system with a range over 2,000 km. They already possess missiles capable of reaching Israel, and some of these have been intercepted by Arrow-3 missiles in the exo-atmosphere.²² Several reasons, beyond the mere pursuit of reliability, might prompt the Houthis to undertake such a development, as the systems used for long-range strikes currently might present various flaws. Firstly, it appears that the delivery systems used by the Houthis may be operating at their maximum range when firing at Israel. It seems possible that they are fired along a so-called Minimum Energy Trajectory (MET),²³ which maximises range. Secondly, it is possible that the Houthis have reduced the weight of the warheads to strike as far as Israel.²⁴ Finally, from an operational perspective, the available information indicates that launches against Israel have been carried out from the country's north-western border (to be as close as possible).²⁵ Although most of the missiles are mounted on TELs,²⁶ which facilitates their deployment, systematically launching from the same area exposes the vehicles to pre-emptive strikes (whether by Israel, the United States or Saudi Arabia). Therefore, the objective is likely to develop a missile with a range equal to or slightly greater than 2,000 km, which could be launched from other areas while maintaining high speed—without the significant speed reduction required in the MET configuration—and delivering a significant military effect, as the payload would not be reduced.

On the third set of queries

The proposals concerning the multi-variant missile family known as the R2000, which is understood to include an HGV, have remained at the conceptual stage. Anthropic provides no further information on this family of missiles, but it is reasonable to assume that the aim is to standardise production lines for propellants, engines, stages, and warheads—for instance, to facilitate production or assembly. The engineering units are clearly striving to achieve operational flexibility and to move away from ballistic trajectories, as suggested by the research into the development of an HGV. This type of vehicle is a technology present in Iran on the Fattah-2, one of the most advanced missiles in the Iranian arsenal. This type of missile architecture, whose warhead and stages could vary according to need, appears to address the challenge of penetrating ballistic missile defence (BMD) systems. Without terminal manoeuvres, exotic trajectories or electronic countermeasures (ECM) most missiles are detected early and intercepted by Israeli or US multi-layered defences.

This body of research appears to be the most concerning. The unit involved is gathering information on the most advanced ballistic technologies. And although the complexity of designing an HGV makes this type of delivery system extremely difficult and time-consuming to develop, this series of enquiries suggests an interest in acquiring and in developing state-of-the-art missiles. The diagram below illustrates the various trajectories that might be under consideration by the Houthis for the R2000 programme. An AN/TPY-2 radar – the primary

²² The first interception by the Arrow-3 also protected Eilat, an Israeli city on the shores of the Red Sea, at the head of the Gulf of Aqaba, more than 1,650 km from Houthi-controlled territory. See Yehoshua Kalisky, 12 November 2023, 'History in the skies: the first operational use of Arrow 3,' *The Institute for National Security Studies*, https://www.inss.org.il/social_media/history-in-the-skies-the-first-operational-use-of-arrow-3/

²³ Which can be roughly summarised as a launch at a 45° angle.

²⁴ In Tsiolkovsky's equation, this means increasing the ratio of initial mass to final mass.

²⁵ 'Yemen's Houthi missile launch centres and the potential targets,' *Sheba Intelligence*, 16 January 2024, <https://www.shebaintelligence.uk/yemens-houthi-missile-launch-centers-and-the-potential-targets>

²⁶ Tractor-erector-launcher.

sensor for the Terminal High-Altitude Area Defense (THAAD), and potentially linked with the Israeli Arrow-3²⁷ – is arbitrarily positioned at the point of impact to demonstrate detection.

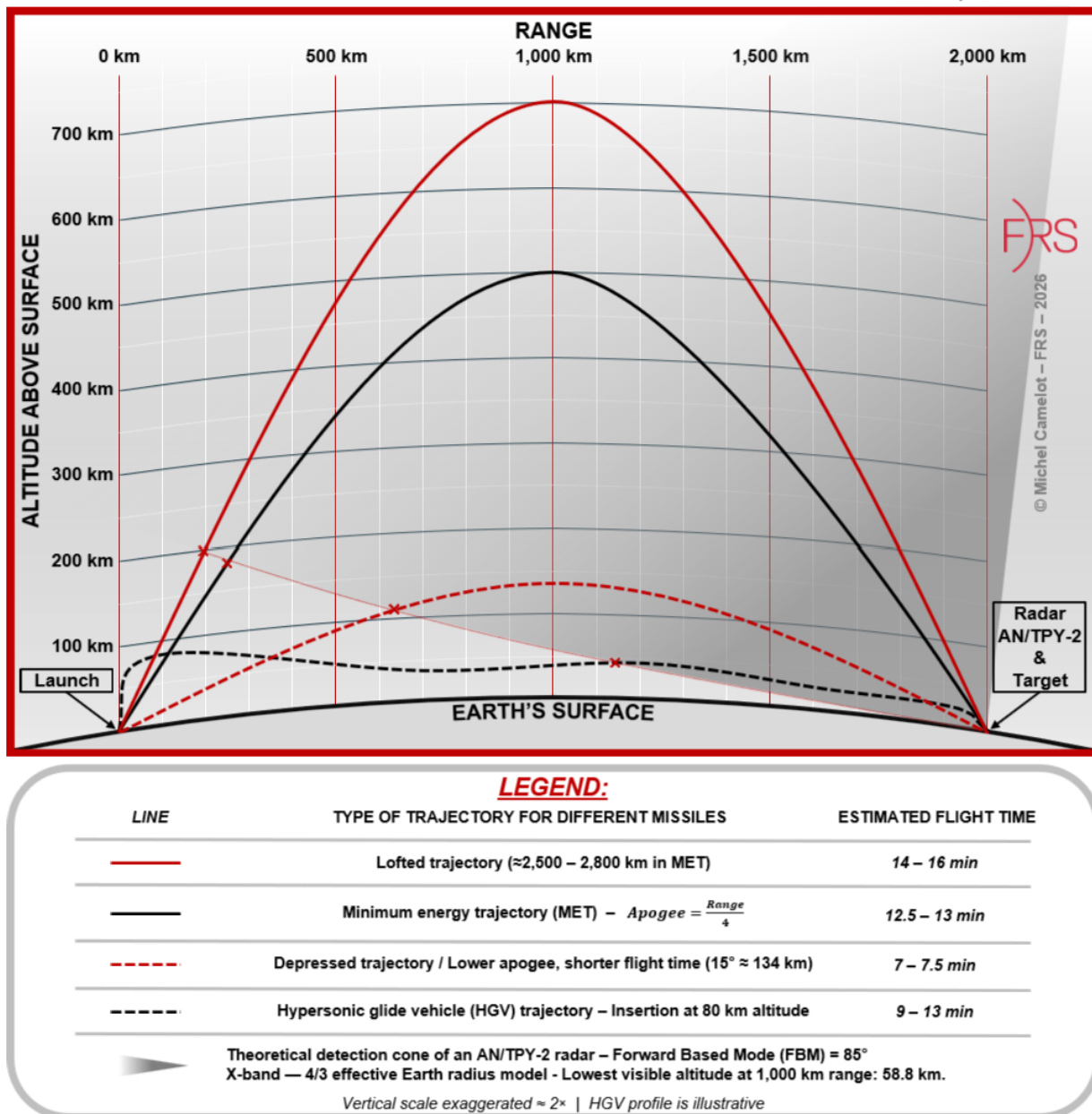


Figure 2 Examples of trajectories for a target at a range of 2,000 km

- The advantage of a depressed trajectory is that it is faster in-flight time. This characteristic makes it suitable for use in pre-emptive strikes against ICBM launch bases to destroy the silos before the launch of retaliatory missiles (This scenario obviously does not apply to the Houthis).
- A lofted trajectory is longer and higher. Such a trajectory may be selected to increase the chance of overwhelming defence, complicate radar tracking and reach the target at very high speed. One of the

²⁷ Masao Dahlgren, 'Israel, United States Test Arrow 3 Interceptor,' 29 July 2019, CSIS, Missile Threat <https://missilethreat.csis.org/israel-united-states-test-arrow-3-interceptor/>

drawbacks of this type of trajectory is that it places the RV (Re-entry Vehicle) under extreme stress, in particular mechanical and thermal, as it decelerates abruptly upon entering the atmosphere. Moreover, Iran has fully mastered these issues at these ranges²⁸.

- An HGV enables flight below the horizon of ground-based radars by gliding through a low-density layer of the atmosphere, at an altitude comprised between 40 and 60 km.

Conclusion

The Houthis already had access to the expertise of engineers from the Yemeni army's Missile Research and Development Centre who had defected to the organisation²⁹ coupled with active technical support from Tehran. Artificial intelligence now offers them the opportunity to accelerate the design, simulation and iteration of ballistic systems with greater software autonomy. Anthropic also points out that the group has developed an offline simulation environment enabling it to test and validate its systems digitally without permanent reliance on online versions.

Programme	Maturity level	Operational benefit
Terminal guidance software on a COTS smartphone	Testing and post-test analysis	GNC optimisation Mass production Circumvention of embargoes
Multi-stage missile $\geq 2,000$ km	Simulation	Increasing range and overcoming the geographical constraints of launches from the north-west Variation in flight profiles
R2000 / HGV ballistic missile family	Conceptualisation	BMD penetration

This gain in autonomy remains, however, only partial. Ballistics is not the only technological bottleneck they may face. Technical and operational mastery of ISR (Intelligence, Surveillance and Reconnaissance) and the entire targeting chain remains very limited and continues to structurally tie the Houthis to Iran³⁰. The strategic value of AI therefore lies not in enabling them to design systems from scratch that they do not know how to manufacture, but in reducing the time between design, testing, identification of a fault and the next iteration.

The rapid design dynamics observed here are not unique to this theatre. The most emblematic example of 'prototype warfare' is currently unfolding in Ukraine, in the race between drones and interception systems. The Anthropic report also mentions that a Russian team was using code from Claude to develop a programme for coordinating swarms of kamikaze drones. These findings raise two distinct policy questions. The first concerns providers of closed models. Since the misuse relied on fragmenting requests across several accounts, detection must operate on aggregated behaviour rather than on individual prompts, and structured information-sharing between providers and governments could help. The second concerns open-weight models (such as Alibaba's Qwen 3.8 or DeepSeek 4.1 and their successors) that can be run locally, where account closures and safeguards are ineffective. Options here are more limited and would need to be examined within existing missile-technology controls and confidence-building frameworks, such as the MTCR and the HCoC, rather than through new, generic regulation of AI.

²⁸ Interview with Stéphane Delory, Senior Research Fellow at FRS, September 2026.

²⁹ Jean Masson, op. cit.

³⁰ Dana Polak and Boaz Shapira, 'How did the return of the "Behshad" to Iran influence the Houthi attacks against ships in the Red Sea,' *Alma Research and Education Centre*, 24 April 2024, <https://israel-alma.org/how-did-the-return-of-the-behshad-to-iran-influence-the-houthi-attacks-against-ships-in-the-red-sea/>

ABOUT THE AUTHOR

Michel Camelot is a Research Fellow at the Foundation for Strategic Research (FRS). He holds a master's degree in International Relations, specializing in international security and defence. His research focuses on defence issues, with a particular emphasis on operational and capability challenges. His work primarily addresses French nuclear deterrence, next-generation missile technologies (including hypersonic systems), and the evolution of drone warfare. In this capacity, he analyses how these technological innovations shape employment doctrines and transform contemporary warfare.

THE HAGUE CODE OF CONDUCT



The objective of the HCoC is to prevent and curb the proliferation of ballistic missile systems capable of delivering weapons of mass destruction and related technologies. Although non-binding, the Code is the only universal instrument addressing this issue today. A multilateral instrument of a political nature, it proposes a set of

transparency and confidence-building measures. Subscribing states commit not to proliferate ballistic missiles and to exercise the maximum degree of restraint possible regarding the development, testing, and deployment of these systems.

The Fondation pour la Recherche Stratégique, with the support of the Council of the European Union, has been implementing activities that aim at promoting the implementation of the Code, contributing to its universal subscription, and offering a platform for discussions on how to further enhance multilateral efforts against missile proliferation.

USEFUL LINKS



www.hcoc.at



www.nonproliferation.eu/hcoc



www.frstrategie.org/



www.eeas.europa.eu



This project is funded by the European Union



This project is implemented by the Fondation pour la Recherche Stratégique.