

Deterrence and NATO's Emerging Security Environment

By

Alex Alfirraz Scheers

The international security environment is deteriorating rapidly and becoming increasingly dangerous and uncertain. China, Iran, North Korea, and Russia pose a threat to Western interests in multiple domains. Among them are economic, conventional, and nuclear, as well as emerging domains such as cyber and space. The Arctic and the deep sea are also areas where they are challenging the West.

These domains and areas are being weaponized for strategic purposes, as adversaries target cross-domain North Atlantic Treaty Organization (NATO) interests with the intent of weakening the Western security architecture and fragmenting alliance cohesion. The Trump administration must work closely with NATO allies to confront the many challenges that face them.

Strategic challenges, such as the Arctic, deep sea, and space, and the threats they pose require improved joint military readiness, enhanced deterrence by denial capabilities, and improved intelligence, surveillance, and reconnaissance.

“Over the last 15 years,” [writes](#) Scott Savits, “the Arctic has become a renewed theatre of military competition.... [T]op Russian officials have referred to the Arctic as Russia’s ‘Mecca,’ and a large fraction of Russia’s economy is based on Arctic fossil fuels and minerals.” Frustrating Russian efforts to gain a strategic advantage in the Arctic is of paramount importance to NATO’s deterrence mission.

Russia gaining an advantage in the Arctic will enhance its ability to establish escalation dominance against NATO in the event of a conflict with the alliance. Deterring Russia from broadening the scope of conflict, by threatening NATO’s vital interests in the Arctic, remains critical in dissuading other adversaries, such as China, from seeking to gain similar advantage.


With China developing and deploying new detection technologies in anti-submarine warfare, American nuclear submarine capabilities are becoming increasingly vulnerable to detection and targeting. China’s “Death Star” satellite claims to possess detection capabilities that renders the [ocean transparent](#) for up to 500 meters beneath the surface, putting American submarines at risk.

In the space domain, it is estimated that loss of access to space would come at a cost of roughly [One billion pounds](#) per day to the British economy. The reported deployment of Russian [anti-satellite weapons systems](#) (ASAT) in space are clearly coercive moves designed to threaten NATO’s space assets.

Russia’s weaponization of space is especially concerning as NATO depends on space to conduct an array of operations across the spectrum of deterrence and defence. Most notably, NATO airpower relies on space-based and space-dependent systems to fulfil a series of critical security functions. Leveraging robust deterrence capabilities in orbit, through targeting Russian and Chinese space-based military and non-military assets, is critical to securing NATO’s vital interests in space.

Beyond seeking strategic advantage, China is also expanding and modernising its nuclear arsenal at an unprecedented rate since the end of the Cold War. The Pentagon forecasts that China will be a [nuclear peer](#) of the United States by 2035. The latest figures published by the Federation of American Scientists show that China now possesses at least [500 operationally deployed nuclear weapons](#)—up 43 percent from [2020](#).

Russian President Vladimir Putin continues to undermine international norms by persisting in threats to use battlefield nuclear weapons in Ukraine. Russia also deploys dual-use satellite technologies in space, capable of carrying nuclear warheads into orbit, in direct



contravention of long-standing international treaties such as the [Outer Space Treaty](#) (1967), which prohibits the weaponization and nuclearization of space.

Meanwhile, Iran, a latent nuclear state, coerces the West by threatening the weaponization of its nuclear program. Iran also infiltrated the West by creating [extremist networks](#) through community centers, [laundering money](#) in major European and American cities that is used by [criminal gangs](#) to plot and execute terrorist attacks.

Proxies supported by Iran, such as Hamas and Hezbollah, can also launch increasingly devastating attacks. Furthermore, attacks like October 7, 2024, or September 11, 2001, do not warrant nuclear retaliation. A nuclear response to a terrorist attack, depending on the attack, is likely a disproportionate response.

China and Russia also engage in subversive activities within the cyber domain, sowing discord by using [disinformation](#), [intellectual property theft](#), and [malign interference](#) to destabilize NATO member states. Cyberattacks on critical national infrastructure can also inflict severe levels of damage. The appropriateness of cross-domain responses is yet to be decided.

The [cyber attacks against Estonia](#) in 2007, which lasted for 22 days, did not result in the triggering of NATO's Article 5 collective defense clause. Yet, it was an attack on a NATO member state. The character of the attack complicated the process by which a viable and appropriate retaliatory response could be devised. In a multidomain threat landscape, hostile state actors conducting their operations in the grey zone can claim plausible deniability.

China, Iran, Russia, and North Korea also hold joint exercises, share intelligence, exchange military capabilities, and share a diplomatic and political kinship. This axis of Western adversaries shares the same geopolitical and economic objectives. They seek to replace the international rules-based order and establish alternative institutional frameworks to global order that undermine concepts such as democracy, human rights, rule of law, and national sovereignty.

Militarily, nowhere is this more apparent than in Russia, where [Iranian drones](#) and [North Korean soldiers](#) were provided to aid Putin's war in Ukraine. Politically, emerging international blocs such as the BRICS demonstrate the extent to which countries like China and Russia are gaining traction in driving alternatives to the current order.

"As hybrid threats evolve to encompass the whole of digital and networked societies," [wrote](#) Sean Monaghan, "so too will the capabilities required to deter them. A more complex threat environment will make predicting attacks and vulnerabilities more difficult, so nations may rely more on resilience."

Hence, for deterrence to be effective today, credibility must incorporate more than hard power capabilities. Red lines must be communicated effectively across different channels. Resolve must be demonstrated through a force posture that includes a willingness to establish escalation dominance in a crisis scenario. The art of deterrence is also about determining and holding at risk what an adversary values.

As the outgoing US Secretary of Defence General (Ret.) Lloyd Austin [said](#) in 2022, cross-domain deterrence "is the right mix of technology, operational concepts, and capabilities—all woven together and networked in a way that is credible, flexible and so formidable that it will give any adversary pause.... [It is] multidomain, spans numerous geographic areas of responsibility, is united with allies and partners, and is fortified by all instruments of national power."

Ultimately, deterrence is about credibly threatening to impose unacceptable costs, by denial or punishment, on a would-be aggressor. Those costs must convince the would-be aggressor that they outweigh any potential gains made.

Therefore, it is imperative for the US and NATO to increase cross-domain capabilities to match those of adversaries. Adopting a combination of different violent and non-violent means, to conduct deterrence credibly across multiple domains and at various levels of intensity, will



enhance NATO's ability to secure its vital interests in an increasingly volatile era of global strategic competition.

Alex Alfirraz Scheers holds a diploma in Politics and History from the Open University, a bachelor's degree in War Studies and History from King's College London, and a master's degree in National Security Studies from King's College London. He has held research positions at the Henry Jackson Society and the International Centre for the Study of Radicalisation, and his articles have been published in the Diplomat, Times of Israel, RealClearDefense, and the Royal United Services Institute. Views expressed in this article are the author's own.