



Emerging disruptive technologies: Dilemmas of deterrence

By Prof. James Henry Bergeron

The issue of emerging and disruptive technologies (EDT) has been trending in the North Atlantic Treaty Organisation (NATO) of late. The 2019 NATO Leaders Meeting in London set out an EDT Roadmap.¹ The NATO 2030 Report cited EDT as a major area for focus and investment. In February 2021, defence ministers agreed in general terms on coordinating investment in EDT, strengthening relationships with private sector innovation hubs and creating foreign export protection mechanisms.² NATO has set a headmark of developing policies on seven key EDT areas: artificial intelligence (AI), data, autonomy, biotechnology, hypersonic technology, quantum physics-based technologies, and space. The ministers also announced plans to complete specific AI and data strategies by summer 2021. The AI Strategy was released in August 2021.³

¹ See: 'London Declaration', North Atlantic Treaty Organisation, 04/12/2019, <https://www.nato.int/> (checked: 09/05/2024).

² See: 'New focus on emerging and disruptive technologies helps prepare NATO for the future', North Atlantic Treaty Organisation, 03/03/2021, <https://www.nato.int/> (checked: 09/05/2024).

³ See: 'NATO releases first-ever strategy for Artificial Intelligence', North Atlantic Treaty Organisation, 22/10/2021, <https://www.nato.int/> (checked: 09/05/2024).



On 1st March 2021, NATO's Advisory Group on Emerging and Disruptive Technologies released its first annual report with recommendations to create an internal agency based on the United States (US) Defence Advanced Research Projects Agency (DARPA) that would group together existing centres, invest in new technology, and collaborate with allied innovation hubs in the public and private sectors. This would be backed by a NATO investment bank to fund innovation in EDT. Those recommendations were approved at the Brussels Summit.⁴ At the 2022 Madrid Summit, the allies established NATO's Defence Innovation Accelerator for the North Atlantic to strengthen transatlantic collaboration on emerging technologies. Twenty three allies also committed to a €1 billion (£860 million) NATO Innovation Fund which began project support last year.

Seen through a NATO institutional prism, an important if understated concern with EDT is its potential disruption of allied cohesion and interoperability. As some move forward with embracing advanced EDT – the US in particular – there is a concern that other allies may not be able to keep up, and that the ability to communicate and operate together at the 'speed of relevance' will be impaired. The alliance's efforts look forward to setting NATO standards and encouraging technology sharing, as well as playing a collective role in fostering innovation.

Seen through a NATO and allied external prism, of course, EDT is seen as a part of 'systemic competition', and particularly for NATO, through the lens of deterrence of aggression. Allied Maritime Command (MARCOM) is engaged in this transformation, particularly in underwater autonomy. Building on the success of the Portuguese-hosted REP(MUS) exercise series, MARCOM established DYNAMIC MESSENGER, an opportunity to incorporate experimentation in underwater autonomy into a conventional exercise. MARCOM has also begun to seriously explore the implications for EDT in the future of naval warfare and alliance security.

EDT has been described in terms of technology advantages to protect and advance, or of challenges to counter, and there is a small but growing literature on the implications of EDT for deterrence. This Primer explores that third dimension, the implications of EDT for deterrence in the concrete situation in which Britain and NATO find themselves.

⁴ See: 'Brussels Summit Communiqué', North Atlantic Treaty Organisation, 14/06/2021, <https://www.nato.int/> (checked: 09/05/2024).

EDT and deterrence

As an opening point, the term ‘disruptive’ in EDT is not particularly useful. All major technological breakthroughs are disruptive of what went before. When Jackie Fisher, then First Sea Lord, built HMS Dreadnought – the first all-big gun battleship – that was certainly an application of disruptive technology. There is a parallel to the use of ‘asymmetric’ in the 2000s as almost a term of abuse. In both cases, a threat was perceived to *status quo* advantages.

Deterrence is usually described as being of two types: deterrence by punishment and deterrence by denial.⁵ The first approach promises unacceptable retaliation should an adversary cross the policy red line which deterrence is intended to prevent. This is a popular notion of nuclear deterrence and it remains relevant at the highest end of conflict. But increasingly over the years, deterrence by denial has achieved emphasis – even prominence – in Euro-Atlantic military circles. For the nuclear powers, the two are linked in ways that foster, if not mandate, ‘grey zone’ or indirect manoeuvre, or an attack only on non-nuclear others, as in Ukraine, as the only feasible major use of the military instrument of power.

This argument rests on the premise that Mutual Assured Destruction (MAD) remains the prime factor in shaping deterrence and defining the limits of ‘competition’ between the nuclear powers and, to a degree, between middle non-nuclear powers tied to nuclear alliances. But what that means for conventional conflict has always been subject to debate. At the height of the Cold War, it was widely assumed that a Soviet invasion of Western Europe would lead to a nuclear exchange between the US and British and Soviet homelands. The shift from conventional to nuclear conflict was viewed as likely to be inevitable. NATO also threatened first use of nuclear weapons if necessary to stop Soviet aggression, even as Moscow does today against NATO, as witnessed several times in relation to Russia’s war against Ukraine.

As early as 1954, Basil Liddell-Hart, the British military thinker, argued that a nuclear weapon would never be used against anything but the threat of another nuclear weapon.⁶ In other words, nuclear competition existed in a sealed bubble and was separate from conventional conflict. If that were true, then the world has, for many decades, been ‘safe’ for great power conventional conflict. Yet, war between the major powers has not broken out and recent history

⁵ The classic work is Glenn H. Snyder, *Deterrence by Denial and Punishment* (Princeton: Center of International Studies, 1959). Also see: André Beaufre, *Deterrence and Strategy* (New York: Praeger, 1965) and Thomas Schelling, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1980).

⁶ See the Preface of: Basil Liddell Hart, *Strategy*, (London: Faber and Faber, 1954).

indicates that the desire on all sides to manoeuvre beneath the assumed escalation threshold, as foretold by George Orwell, is as strong as ever.⁷ Why? Arguably, due to uncertainty on all sides that conventional conflict would not escalate out of control, combined with the lack of truly vital national interests being challenged. But as a result, deterrence needs to be considered in the systemic context of mutual deterrence, a deterrent equilibrium, possibly even competitive deterrence.

In a situation where a major nuclear exchange would still destroy the belligerents and much of the world, manoeuvre strategies for advantage, beneath the believed threshold of kinetic escalation between nuclear states and alliances, are pursued as a form of political or strategic capital in pursuit of important national interests. The cyber and electronic warfare realms, hypersonics, space, AI, data, autonomy, and quantum technologies are all becoming primary fields for this activity.

Does the emergence of EDT destabilise or undermine prevailing assumptions about the viability of deterrence, as well as the role of deterrence in peacetime or 'grey zone' times? There is a growing literature on this. Recently Brad Roberts provided an excellent review of EDT scholarship, noting that scholars profoundly disagree over the deterrent impact EDT will have.⁸ Further, studies of the role of EDT in conflict tend to dominate the literature.⁹ Explorations of its use in crisis management are fewer and EDT in peacetime rivalry is the least developed field of all.¹⁰

What deterrence requires

The practical application of a deterrent strategy in the contemporary era has depended on a few key factors. Deterrence requires a mutually understood sphere of activity by an adversary that is acceptable, even if unwelcome, and a sphere that crosses the 'red line' into triggering a response. Ideally all sides share a strategic appreciation of where these lines exist. Things get harder when strategic appreciations differ.

⁷ See: George Orwell, 'You and the Atom Bomb', *Tribune* via The Orwell Foundation, 19/10/1945, <https://www.orwellfoundation.com/> (checked: 09/05/2024).

⁸ Brad Roberts, 'Emerging and Disruptive Technologies, Multi-domain Complexity, and Strategic Stability: A Review and Assessment of the Literature', Centre for Global Security Research, 17/03/2021, <https://cgsr.llnl.gov/> (checked: 09/05/2024).

⁹ *Ibid.*

¹⁰ *Ibid.*

Deterrence requires knowledge of adversary capabilities. Recall Dr Strangelove's response to the Soviet ambassador on the Doomsday Machine which the USSR kept secret: 'Why didn't you tell us?' This is the first essential dilemma of the era of EDT for deterrence. With new technology, there is a motivation to surprise as well as the desire to deter. A compromise between these goals might involve broadcasting successes in some EDT fields, while holding others back. Directed energy weapons and hypersonics might fall more easily into the first category, while AI, data, cyber, space, electromagnetic pulse (EMP) employment and quantum breakthroughs might better fit the second. But the tension remains, evidenced by the November 2021 Russian destruction of a satellite in orbit, demonstrating a key capability.¹¹

This also raises the distinction between the application of EDT in 'peacetime' or non-crisis situations, and their employment at the point of crisis-to-conflict. The dynamics are quite different. In grey zone manoeuvre, surprise is not the aim, the purchase of political capital is, at the expense of signalling a capability (or intent to acquire one) and allows a potential adversary to work on a counter. The Russian satellite shoot-down is enlightening here. By contrast, the application of EDT as a strategic shock in crisis may have operational advantages, possibly decisive ones, but also risks losing control of escalation. There was a notable NBC report on 24th February that Joe Biden, President of the US, had been briefed on major offensive cyber options against Russia as the war in Ukraine was beginning.¹² The White House immediately rejected the claim as 'wildly off base'.¹³ It may well have been, but the episode also illustrates the difficult linkage between surprise and escalation with EDTs.

Deterrence depends on time. There needs to be enough time to process decision-making through the adversary's administrative and political processes, but not so much time that they can offer counter-strategy for escalation. And not so little as to force a 'use it or lose it' response.

Further, systemic deterrence requires a relationship between time and counter-strategies that encourages restraint now in hopes of reversing the deterrent advantage in the future. There is an 'Observe, Orient, Decide and Act (OODA) loop' effect where each side chills action by the other, all seeking advantage, the technology takes time to develop and deploy, and the challenges are chronic enough for long-term strategic decision making. They do not arrive so quickly or in such numbers to prevent a deterrent counter-strategy; they do

¹¹ 'Russian anti-satellite missile test draws condemnation', *BBC*, 16/11/2021, <https://www.bbc.co.uk/> (checked: 09/05/2024).

¹² Ken Dilanian and Courtney Kube, 'Biden has been presented with options for massive cyberattacks against Russia', *NBC News*, 24/02/2022, <https://www.nbcnews.com/> (checked: 09/05/2024).

¹³ 'White House denies report on Biden being presented with cyberattack options against Russia', *Reuters*, 24/02/2022, <https://www.reuters.com/> (checked: 09/05/2024).



not take so long that one believes they have an enduring advantage. This takes the form of effective competition over innovation, production, and military posture for deterrent advantage.

Application to the era of EDT

Applying this thinking to EDTs – a few case examples raise interesting questions for deterrence:

1. **Command and control:** As Chris Dougherty points out, wargame after wargame of US–Russia and US–People’s Republic of China (PRC) confrontations posits the conflict to begin with an attack on command and control (C2) to disassemble the effectiveness of the command structure and sever the links with deployed forces.¹⁴ There is a first mover advantage here, especially where a first mover like Russia also seeks to adopt a short-war strategy, a one–two week conflict window followed by a negotiated settlement in their favour.

Implications of EDT here are mixed. In the grey zone, it does not appear that the use of cyber disruption in non–crisis situations breaks the deterrent threshold for a kinetic response, so long as the damage resulting is itself data and not physical damage. Consider SolarWinds.¹⁵ Does ‘what happens in Cyber stay in Cyber’? The Colonial Pipeline software hack could have been the limiting case here with its resulting shutdown of the pipeline by Colonial as a precaution, but it was not.¹⁶ The attribution problem was in play, with the US Government pointing the finger at Russian cyber–criminals, but not the Kremlin. In the crisis or acute situation, the result could be different. Physical retaliation might be more likely if an attack was against dual use command, control and communication (C3I) systems, where a debilitating strike could have both conventional and nuclear response implications.

Location also matters. In the grey zone, an element of protection seems to exist in the reluctance of great powers to strike each other’s homelands. But that could be less of a concern with C2 nodes based

¹⁴ Chris Dougherty, ‘More than Half the Battle: Information and Command in a New American Way of War’, Centre for a New American Security, 20/05/2021, <https://www.cnas.org/> (checked: 09/05/2024).

¹⁵ ‘SolarWinds hack was “largest and most sophisticated attack” ever: Microsoft president’, *Reuters*, 15/02/2021, <https://www.reuters.com/> (checked: 09/05/2024).

¹⁶ David E. Sanger and Nicole Perlroth, ‘Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity’, *The New York Times*, 14/05/2021, <https://www.nytimes.com/> (checked: 09/05/2024).



elsewhere. Dougherty tells of a wargame where air C2 was relocated from US Air Forces Europe to the continental US to raise the stakes for pre-emption and retaliation.¹⁷ There is also a logic in dispersing C2 across the territory of several allies, as with the NATO Command Structure, to confound attempts by an adversary to focus its attack and limit the conflict. Interestingly, that protection might be at its weakest in deployed command and control systems aboard ship or in the air in the global commons.

There is also a human dimension to C2, and an aspect of EDT that has not been much addressed. This is the ‘Havana Syndrome’ reports of US State Department and other officials falling ill with numerous debilitating and long lasting symptoms. Little is known (or acknowledged) by governments, although the US Central Intelligence Agency has issued an interim report discussing most cases but considering foreign involvement in about two dozen incidents since 2016.¹⁸ From public sources, it appears that the likely explanation of the most suspicious cases is some form of microwave radiation targeting the individuals in civilian environments. Most of the literature points the finger of suspicion at Russia, although governments have yet to attribute blame.

‘Havana’ attacks differ from cyber attacks or AI-enabled disruption of headquarters. Like bioweapons – as with the Skripal case in the United Kingdom (UK) – this is a kinetic attack on people in a national territory. It crosses the red line for a response, although not necessarily a military response. That may be partly due to the unwillingness or inability of governments to respond in kind to such an unorthodox and illegal form of attack.

There is also the knowledge and attribution problem again, as with cyber and AI-disruptions. The second essential dilemma of EDT for deterrence is the tension between signalling ownership of an ‘attack’ or even a capability for an attack, to benefit from its deterrent effect, and not providing so much evidence that attribution, retaliation, and escalation inevitably follows. The middle ground arguably pursued by the Kremlin in Crimea, Ukraine, with the Skripals and other ill fates met by former spies, SolarWinds, and other hacking efforts, might be called ‘implausible deniability’. The political benefit of such acts requires that the adversary does attribute the act to the antagonist, but not too easily or clearly or formally.

¹⁷ Chris Dougherty, ‘More than Half the Battle: Information and Command in a New American Way of War’, Centre for a New American Security, 20/05/2021, <https://www.cnas.org/> (checked: 09/05/2024).

¹⁸ ‘CIA says “Havana Syndrome” not result of sustained campaign by hostile power’, *NBC News*, 20/01/2022, <https://www.nbcnews.com/> (checked: 09/05/2024).



A diplomatic dimension of such pseudo-ambiguous strategies also exists: implausible deniability creates ‘wiggle room’ where states or parts of an alliance are not keen on a confrontation and are looking for a plausible or face-saving reason not to respond. ‘We can’t be sure’ works well as a strategic communications play in this regard, even if inside government they are relatively sure who the culprit is.

- 2. Autonomous systems and drones:** There has been a revolution in land warfare over the past few years, or perhaps it would be more accurate to call it a new form of air-land battle: the remarkably successful applications of drones on the battlefield in Syria, Libya, the recent Azerbaijan-Armenia conflict, and Ukraine. Their use has also been witnessed in the Middle East and the Gulf. In the land domain, the impact on deterrence does not appear to be very great, as these forces were deployed in conflicts which were ongoing. They changed the tactical picture and perhaps the operational outcome, but did not alter or undermine strategic deterrent effects, although these were not contests between nuclear powers. One potential counter-example is Russian anger at Turkish drones sold to Ukraine and used to respond to insurgent attacks across the line of control in the Donbas.

The situation may be different at sea or in the air, and when used outside of an existing conflict. Ukraine has been remarkably successful in using unmanned surface vehicles, unmanned aerial vehicles and missiles to drive Russia’s Black Sea Fleet out of the western Black Sea, even threatening Sevastopol. Of course, that is a war between a nuclear power and a non-nuclear power. How does the dynamic play out between nuclear states and their deterrent thresholds, pursuing grey zone strategies?

It has been argued that autonomy may allow nuclear peer competitors to take escalatory risks they otherwise would not, given the lack of human lives at stake.¹⁹ But this dynamic cuts both ways – the adversary may also be ready to act against autonomous systems in ways they would not consider against a piloted aircraft. If that is so, there may be a deterrent equivalence at play, almost parallel to Liddle-Hart’s remark about atomic weapons, and some conclusions from non-kinetic cyber-attacks. Are drones and autonomous systems ‘fair game’ for action by great powers on the shared understanding that this exists below the threshold of escalation? In what one might call the ‘Vegas’ effect of some

¹⁹ Michael C. Horowitz, Paul Scharre, and Ben FitzGerald, ‘Drone Proliferation and the Use of Force: An Experimental Approach’, 03/03/2017, Centre for a New American Security, <https://drones.cnas.org/> (checked: 09/05/2024).



forms of EDT, does what happens in unmanned stay in unmanned? Practice is not yet firm on the point, but there are hints in that direction.

3. **AI, mass and speed:** The application of AI can be expected to have divergent effects on the deterrent balance, depending on the nature of the systems being enhanced. An AI or autonomy-enhanced mine clearance capability favours the defence and arguably bolsters deterrence by denial. So do anti-submarine warfare gliders or underwater acoustic sensors, as well as the development of quantum-based radars which might pierce the oceans. But equally, AI and autonomy might also enable 'chaff', a bewildering number of false contacts hiding the real mine or the actual submarine. One might hypothesise that greater transparency, detection or autonomy, in and of themselves, are not destabilising for deterrence, although they might alter the balance of military power.

By contrast, AI-enabled hypersonic weapons or cruise missiles tend to favour the offence. They dramatically shorten the time for response, putting a strain on decision-makers, particularly in large alliances. Their potential dual nuclear or conventional nature creates a problem for knowledge as well as time, which can foster 'use it or lose it' first strike responses if one party believes that the other has deliberately crossed the threshold of aggression. This means that in conflict countries can win faster, but they can also lose faster.²⁰ It is argued that the speed factor is destabilising for deterrence.

However, the other side of AI is its potential automaticity. To turn again to *Dr Strangelove*, the perverse logic of the film's Soviet Doomsday Machine was that computers and sensors would automatically respond to an attack: it removed the human factor from a retaliatory response. In current conditions, adversaries will always consider the coherence of opposing C2 and the willingness of governments, administrations and the military to carry out nuclear orders from the top. Those dynamics do change when the C2 chain is simplified. In one sense, deterrence may be strengthened if there is less scope for C2 breakdown. Alternatively, some important political, military and human checks and balances against first nuclear use may be weakened.

²⁰ Michael C. Horowitz, 'When speed kills: Lethal autonomous weapon systems, deterrence and stability', *Journal of Strategic Studies*, 42:6 (2019), p. 782.

Implications for deterrence and the grey zone threshold

Looking at the problem from the perspective of the grey zone in which the great powers find themselves – arguably confined up until now – does EDT disrupt or destabilise the system of deterrence? And if so, in whose favour?

As this era of EDT is relatively new, it is hard to draw conclusions. But the following may be emerging:

What has been seen to date is a tendency towards parallelism in deterrent posturing relating to EDT, not crossover or horizontal escalation. Non-kinetic and non-human attacks seem to imply non-kinetic and non-human responses. The wild card may be at the individual human level, whether biological and electronic warfare based, where the individual nature of attacks has led to a characterisation more akin to secret service activities and public responses (or non-responses), rather than state on state conflict. Thus, nuclear weapons for nuclear weapons, cyber for cyber, and possibly a growing willingness to attack each other's drones. This is not a disruption of the escalatory threshold so much as a reimagining of what exists below it (EMP could be the exception here).

Certain aspects of EDT do challenge stable deterrence. These include the shortening of decision-making cycles with hypersonics and machine learning, the risk of a perishable first mover advantage in the use of AI, cyber or quantum technologies to disable C2, disaggregate the force and deny (particularly to the UK and US) its current advantages in all domain force integration. At present, however, all players in this technological competition have a reasonable shot at success. Overmatch across all of these fields is not preordained for anyone. As a result, it is probable that the great powers will not abandon their escalatory thresholds in the short or medium term by the lure of an EDT advantage alone, even if any of them could claim it. That advantage is likely to be short-lived, in any case. The perverse implication is that strategic stability in an EDT era is maximised if none of the main players succeed too well or fail too badly.

Last, there remains scope for mutual restraint and the equivalent of arms control-like agreements to suppress some of the more destabilising aspects of EDT. That will not be easy, however. Different powers may see themselves as having advantages or lead times that they might not want to sacrifice. Verification poses daunting challenges. And the proliferation of such technologies beyond the nuclear club of nations will make it very difficult to negotiate restraint short of wide multinational conventions similar to the Chemical or Biological Weapons Conventions.

Conclusion

Ultimately, the foundations of deterrence appear to remain relevant, although the variables may be changing, or afforded differing weights. Deterrence remains concerned with the comprehensive impact of all military capabilities that shape an adversary's risk calculus. It is always to be measured from their perspective. Note that they therefore have an uncomfortable leverage on the purse strings of allied defence budgets and spending priorities.

From a NATO perspective, AI and machine learning may be the biggest institutional challenge. As foreshadowed by Ballistic Missile Defence, the speed of response required in an AI-enabled conflict would shorten the scope for complex political negotiations and compromises that are at the heart of alliance politics. That strikes at allied cohesion, which is a central element in deterrence for NATO. But it is not a new one: at the height of the Cold War, the North Atlantic Council was expected to meet within one hour if necessary to authorise Article 5 collective defence responses to a Soviet attack.

There are some solutions. One would be to follow the Ballistic Missile Defence model and shift politics onto pre-agreed authorisations, metrics, and criteria for the use of force in defence against, or responding to, an AI-enabled or hypersonic attack, or the crippling of C2 systems. The level of delegation required to be effective could be extremely high, possibly down to the combat centre of a warship, and possibly beyond that, taking the human out of the immediate response loop entirely. This level of automation might enhance deterrent credibility but needs to be balanced against effective constraints on irrational or impulsive nuclear use. A second option would be the tacit acceptance that only a few allies, at present, are capable of operating in most EDT environments and would be the first responders. The third option, as promoted in the NATO 2030 report and being pursued in Brussels, is to work on ways to agree on sharing of EDT and counter-EDT capabilities and techniques as widely as possible within NATO. This would ensure a more united and cohesive alliance.



About the author

Prof. James Henry Bergeron is a Distinguished Fellow at the Council on Geostrategy. He currently serves as Political Advisor at Allied Maritime Command. He has served as a foreign policy advisor to ten senior American and NATO Commanders in the fields of maritime and joint expeditionary operations, including as the advisor to Naval Striking and Support Forces in NATO. He is regularly consulted on NATO maritime strategy, NATO-EU relations, and was one of the drafters of the Alliance Maritime Strategy.

“ Dedicated to making Britain, as well as other free and open nations, more united, stronger and greener.

ISBN: 978-1-914441-68-4

Address: 14 Old Queen Street, Westminster, London, SW1H 9HP

Phone: 020 3915 5625

Email: info@geostrategy.org.uk

© 2024 Council on Geostrategy

Disclaimer: This publication should not be considered in any way to constitute advice. It is for knowledge and educational purposes only. The views expressed in this publication are those of the author and do not necessarily reflect the views of the Council on Geostrategy or the views of its Advisory Council.

Please do not print this document; protect the environment by reading it online.

Geostrategy Ltd., trading as Council on Geostrategy, is a company limited by guarantee in England and Wales. Registration no. 13132479. Registered address: Geostrategy Ltd., Lower Ground Floor Office, 231 Shoreditch High Street, London, E1 6PJ.