Disruptive technologies and nuclear risks: What’s new, what matters,

and the way ahead

Andrew Futter[[1]](#endnote-1)

The impact of disruptive technologies on nuclear risks is not new, but we appear to be living through a period of enhanced hype and fear about how certain technological developments are impacting the current nuclear order. New hard and soft weapons systems and support facilities, potential vulnerabilities and associated destabilising dynamics, could all place considerable strain on the global nuclear balance and accompanying architecture. The aim of this article is to examine five disruptive dynamics, explain their intricacies and nuances, and put them in political and strategic context. By doing this, the paper argues that while the nature of nuclear risk is changing (in many cases for the worse), and there are a number of pressures which could have significant negative implications for escalation, stability and order if left unchecked, this phenomenon remains fundamentally political, and there are political mechanisms which can help in both tailored and broader risk reduction. Therefore, while the risks posed by disruptive technologies in the nuclear space are real and growing, they should not be insurmountable.

**Introduction: Towards a more dangerous nuclear world?**

We are entering a more complex chapter of our nuclear story where new technological developments, both in terms of weapons systems and the broader environment, are changing the nature of nuclear risks.[[2]](#endnote-2) This has been interchangeably labelled as the “new”, “emerging” or “disruptive” technology challenge, and often a combination of all three, which has sometimes meant that this debate lacks coherence and clarity. What we can say is that, faster, more precise, and often dual use and intangible weapons, increasingly sophisticated sensing, tracking and processing capabilities, the potential for greater autonomy in these systems across all domains, as well as the myriad possibilities and vulnerabilities presented by computer network operations and non-nuclear counter-space capabilities are questioning many of the central axioms upon which nuclear order, stability and risk reduction are based. These dynamics not only potentially reopen the question of counterforce strikes and deterrence by denial, undermine mutual vulnerability as a central ordering mechanism in nuclear politics, create new conceivable and more complex pathways toward escalation, further blur the nuclear-conventional distinction, and seem likely to inculcate a more suspicious and fearful nuclear environment, but also raise fundamental questions about the political and normative mechanisms required to maintain stability and peace. From the current vantage point this technological onslaught seems set to revolutionise the way that we understand nuclear politics.

For sure, we should be concerned about this emerging nuclear picture, and especially the risks of sleepwalking into what seems likely to be a much-changed nuclear world, particularly from that of the Cold War when the central tenets of nuclear order were conceived[[3]](#endnote-3), but also perhaps from the more recent “Second Nuclear Age” that some have suggested we have been living in since the early 1990s.[[4]](#endnote-4) But to suggest that these challenges are insurmountable or inevitable is to fall into the trap of technological determinism, rather than to focus on the fact that these are political problems, often-though not always-with political solutions or at least remedies. It is also important not to get to focussed on the “new” aspect of this challenge: many of the dynamics that fall under the disruptive technology moniker have either been around for a while, or they effectively provide new tools and mechanisms for old established problems and risks. Likewise, this isn’t the first time that technological challenges to established nuclear thinking, or perhaps more importantly the perceptions of a technological transformation of nuclear order, have caused concern.[[5]](#endnote-5) This all suggests that at least some of these developments could be more marginal than feared, and that perhaps with sufficient political will, this potentially more unstable nuclear era can be managed. The key to our techno-nuclear future will therefore be the primacy of politics over technology.

This article proceeds in five sections: the first considers the notion that certain nuclear delivery systems might be becoming more vulnerable to pre-emptive attack; the second explores the significance of the development and deployment of hypersonic weapons; the third explains how left of launch capabilities could transform the nature and consequences of ballistic missile defence; the fourth unpacks the risks and rewards of AI and Autonomy in the nuclear realm; and the fifth investigates how a more complex nuclear environment driven by developments in both hard, tangible and observable weapons, as well as soft, intangible and difficult to measure capabilities are creating new pathways for nuclear escalation. The conclusion argues for the primacy of politics and begins to outline the way ahead.

**Are mobile missiles and nuclear-armed submarines becoming more vulnerable?**

Deploying nuclear weapons on silent submarines hidden somewhere in the depths of the ocean, or on land-based mobile platforms able to move along roads and rails and hide and only re-appear when needed, has underpinned nuclear order and particularly deterrence thinking for decades. The idea is that if an opponent doesn’t know for certain where these delivery systems are, they cannot be reliably targeted in a surprise first-strike. Thus, logic suggests that no rational actor would risk attempting an attack because of the risk of devastating retaliation. This is the basis of mutual vulnerability and stability through survivable second-strike forces.

While there is reason to believe that some submarines and mobile land-based missiles may not have been as invulnerable in the past as conventional wisdom suggests[[6]](#endnote-6), the reality is that the technical support infrastructure didn’t exist to reliably track and destroy these systems at all times with any great confidence, even with nuclear weapons.

But today significant advances in remote sensor technologies, more capable surveillance platforms across different domains, the ability to process and communicate enormous amounts of data quickly, and more precise non-nuclear and non-kinetic weapons systems, could be closing the gap between “the hiders and the seekers”.[[7]](#endnote-7) Real-time imaging, ultra-sensitive acoustics, and other data could be gathered by a variety of different, possibly stealthy sensor platforms (under the ocean, in space, and possibly uninhabited), sophisticated algorithms (possibly using Artificial Intelligence) could be used to filter the data, and precision-guided weapons systems (or computer network operations[[8]](#endnote-8)) could be used to attack or at least compromise submarines or mobile missiles. This potential ability to target submarines and mobile missiles lays at the heart of what Keir Lieber and Daryl Press have termed as the “new era of counterforce.”[[9]](#endnote-9) If submarines and mobile missiles are becoming more vulnerable to attack (or at least confidence is reduced in their inviolability), then this poses some significant questions for military planners and potentially for deterrence and stability.[[10]](#endnote-10)

However, this is far from a one-size-fits-all problem: not all nuclear-armed submarines and mobile missiles[[11]](#endnote-11) are becoming vulnerable to the same degree. As has been noted elsewhere, the extent of this challenge depends on; whose missiles and submarines are being targeted, where they are located, and who is doing the finding and attacking.[[12]](#endnote-12)

Some nuclear-armed submarines for example, (notably those operated by the US and UK) are believed to be much quieter than the submarines deployed by other nations, they are therefore more difficult to locate through purely acoustic measures. US and UK submarines are also probably harder to track than Russian or Chinese submarines when they leave port, and while patrol areas may be limited by underwater mapping or missile ranges, these submarines can still hide in many millions of square miles of ocean (which in turn would place enormous strains on the number, endurance and capability of systems used to track them).[[13]](#endnote-13) That said, any advances in anti-SSBN warfare capabilities would be particularly acute for the UK given that it is the only nuclear-armed state that relies on just one form of nuclear delivery.

In terms of mobile missiles, China and especially Russia have huge interior spaces in which to hide and move their missiles (albeit this may be limited by the extent of road or rail networks), and of course a lot of missiles. The task of tracking mobile missiles might be easier in a smaller country with less strategic depth, but it would still be difficult to attack before they could be launched and to do so with confidence. This would be particularly challenging if conducted with non-nuclear precision weapons, even terminally guided, given the extreme accuracy required. Moreover, knowing the precise location of a mobile missile at all times is difficult. In theory satellites could provide constant surveillance of particular areas where mobile missiles are thought to be deployed, but in reality, this would take lots of satellites in many different orbits.[[14]](#endnote-14) Achieving similar levels of surveillance with UAVs might be an option, but UAVs are more vulnerable than satellites given that they would probably have to be much closer to the target, flying through or even loitering in enemy air space.

The “seekers” also have to contend with countermeasures. This may include deploying dummy mobile missiles so that it becomes difficult to discriminate between real and false targets. Submarines may deploy countermeasures to confuse sensors, and any underwater sensing or weapons platform would presumably be vulnerable to attack too. Submarines may also be moved in protected “bastions” closer to the shore beyond the reach of an adversary’s underwater systems.[[15]](#endnote-15) Moreover, while finding and tracking missiles or submarines would be one thing, having the required munitions close enough and able to attack them would be another. This is not to say that some targets could become more vulnerable, and perhaps, vulnerable to a non-nuclear strike in this inherently fluid strategic picture. Specifically, the US could probably target North Korean mobile missiles (such as the recently unveiled Hwasong-15), and indeed, this may have been contemplated during periods of high tension in the recent past.

The ability to find, track and strike mobile missiles and submarines requires significant investment and infrastructure, and of course political will. Indeed, perhaps the most important factor limiting the counterforce potential of new technologies will be the desire to pursue such options. Just because something might be *technically* feasible, doesn’t mean it makes *political* or *strategic* sense.

Fears of a more transparent ocean or surgical attacks on land-based nuclear delivery systems will continue to drive modernisation and maybe even arms racing. In this way, it is as much about perceptions and uncertainty regarding future technological breakthroughs as about what is happening now. Thus, if we are entering into a new era of counterforce, it will one inhabited primarily by the United States, at least for the foreseeable future, and one where only some countries nuclear systems may be more vulnerable in certain extreme scenarios, not necessarily all.

**How destabilising are hypersonic missiles?**

Perhaps no development better encapsulates the disruptive technology thesis than hypersonic weaponry. Images of futuristic-looking projectiles or aircraft, glowing red due to the enormous heat produced by manoeuvring through the atmosphere at high speeds, and able to strike targets with high-precision seem to embody this new paradigm. Such weapons will purportedly be able to travel extremely quickly, evade missile defences, reduce warning times due to their trajectory, and manoeuvre in flight to hit specific targets anywhere in the world. Hypersonic weapons are being developed by all major nuclear-armed states, and concerns of arms racing have ensued.[[16]](#endnote-16)

Hypersonic weapons are classified by the speed at which they travel–hypersonic, or Mach 5 and above, which is roughly one mile per second.[[17]](#endnote-17) Current systems can be split into hypersonic glide vehicles (HGVs), which are launched from booster rockets before gliding unaided across the top of the atmosphere and falling to their targets, and hypersonic cruise missiles (HCMs), which are powered, air-breathing, and stay inside the atmosphere.[[18]](#endnote-18) Each system presents different prospective benefits: HGVs potentially offer greater manoeuvrability and less predictable flight paths than current ballistic missiles, making them better at avoiding interception by mid-course ballistic missile defences, while HCMs retain the accuracy and manoeuvrability of subsonic (slower than the speed of sound) or supersonic (faster than the speed of sound) cruise missiles but at much higher speeds (and higher altitudes). HGVs and HCMs are therefore probably better thought of as variations of current ballistic and cruise missiles rather than something entirely new.

Hypersonic weapons could be used for a number of different military objectives: delivering nuclear or non-nuclear weapons, destroying mobile missiles, anti-satellite weapons, radar installations, missile defence assets, ships or other high value targets. To highlight the point, the US, Russia, China and India all have slightly different purposes for their respective programmes. The US appears to see HGVs and HCMs as part of a broader *conventional* global prompt strike mission and doesn’t currently seem interested in developing nuclear-armed hypersonic weapons.[[19]](#endnote-19) Russia (whose interest in hypersonic technology can be traced back to the 1980s[[20]](#endnote-20)), seems to be building hypersonic missiles, specifically the Avangard HGV, for the long-range delivery of nuclear weapons, and as a direct response to concerns about US ballistic missile defence plans. For China, hypersonic developments focus on regional Anti-Access Area Denial, and principally targeting an adversary’s forces at sea (e.g., with the medium range DF-17 missile), but interest in long-range HGVs are being driven by growing fears of US surgical strikes against nuclear assets.[[21]](#endnote-21) It is not yet clear whether these systems will be nuclear or conventional. India appears to be developing HCMs, notably the Brahmos-II (in partnership with Russia), which may be nuclear-capable, to enhance regional deterrence against China and Pakistan.[[22]](#endnote-22)

Hypersonic weapons pose a range of (heightened but not necessarily new) nuclear risks due to three “ambiguities”.[[23]](#endnote-23) First, the inability to know the intended *destination* of the warhead due to the unpredictable flight path means that it *might* be less clear which country is under attack than with ballistic missiles. Second, it could be difficult to know which *targets* are under attack, i.e., nuclear weapons facilities, a non-nuclear military installation, or a “soft” target such as a city, and therefore to discern the intention of the attackers. In some cases, this isn’t very different from ballistic missiles. Third, is the inability to know whether the *warhead* is armed with a nuclear or conventional warhead. While this is comparable for ballistic missiles, the possibility of using the same hypersonic delivery systems for nuclear and non-nuclear weapons could create confusion, especially if both types of system are deployed together. All of these dynamics seems set to exacerbate the security dilemma, increase chances of inadvertent escalation, and make crisis management more difficult.

These concerns notwithstanding, there are some important limitations to hypersonic weaponry that might prove important in future development, and particularly for arms control. [[24]](#endnote-24) Perhaps most significant is that HGVs don’t offer many military advantages over current ballistic missiles. This is because most ballistic missiles already travel at hypersonic speeds, can have a degree of manoeuvrability (MARVs for example[[25]](#endnote-25)), could be terminally guided to increase accuracy, and might be flown at depressed trajectories to reduce warning time.[[26]](#endnote-26) It is also because current ballistic missiles can probably penetrate-or at least overwhelm-most ballistic missile defences deployed or in development today, especially if they are armed with countermeasures. Moreover, HGVs are likely to be travelling much slower than ballistic missile warheads when they reach their target (they lose speed in flight depending on how much they have manoeuvred) and could be more susceptible to terminal missile defences.[[27]](#endnote-27) HGVs and HCMs will also produce enormous amounts of heat as they cut through the atmosphere, which could make them easier to track with space-based sensors than a normal ballistic warhead or cruise missile. Perhaps above all, successful hypersonic flight is technologically difficult: mastering scramjet propulsion for HCMs, mitigating the effects of extreme heat, and finding a reliable and secure way to comminate with the warhead are all significant engineering challenges. All of these factors could mean that deployment is limited.

When scrutinised, hypersonic weapons appear to offer relatively few military or strategic advantages over ballistic or cruise missiles, or other precision strike capabilities, either for tactical missions or strategic roles. This suggests that it is as much geopolitics and a sense of grandeur that that is driving the apparent fascination with such capabilities amongst the major powers as it is the pursuit of a genuinely transformative weapon system.

However, HGVs and HCMs may be potentially more destabilising and escalation prone than ballistic and cruise missiles. The concern here is far less about the use of hypersonic weapons for nuclear counterforce operations (although this might be feasible in certain scenarios), but rather the potential for miscalculation and misperception through their use in conventional operations.[[28]](#endnote-28) This is especially troubling when hypersonic weapons that could be armed with both nuclear and non-nuclear payloads are deployed together or at least in close proximity.[[29]](#endnote-29)

Managing these risks will involve balancing the demands of conventional warfare with the need to retain nuclear stability.[[30]](#endnote-30) This might mean political limits on deployment (HGVs could also be included under New START and any follow on treaty given that they would rely on similar if not identical launchers to ballistic missiles), a clear geographical separation between the systems used to deliver nuclear and conventional weapons, and greater transparency about the types of weapons being deployed. This could mirror the arms control thinking that helped reduce the risks posed by the indistinguishability of nuclear and conventional ballistic missiles in the past.

**How significant is left of launch ballistic missile defence?**

Since the 1960s, the deployment of active defences against ballistic missiles has been considered as destabilising or disruptive to nuclear order, but two developments appear to be exacerbating this. The first is the deployment and spread of active missile defences of ever-greater capability for kinetic and non-nuclear interception of both nuclear and conventionally armed missiles (we can think of these systems as “right of launch”). The second, is a shift in thinking towards “full spectrum missile defence” that incorporates “left of launch” operations (that is, actions designed to prevent missiles from being launched, such as through computer network operations or electronic warfare). These developments may be making BMD more capable and credible against certain types of missile threats. But they are also increasingly blurring the distinction between defence and offense and between protecting against nuclear and conventional threats, potentially increasing the ability to achieve deterrence by denial (rather than punishment) and creating new concerns about stability.

Right of launch missile defence involves trying to intercept a missile *after* it has been launched. Shooting down a ballistic missile while in flight is technologically demanding, but the difficulty is contingent upon the speed of the missile, how may missiles/warheads need to be intercepted, whether it/they are armed with countermeasures, and the type of interception method being used. Historically, the preferred method of interception was by a nuclear blast as this did not require great accuracy to destroy incoming warheads (and Russia still deploys nuclear-armed interceptors to defend Moscow), but more recently attention has turned to “hit to kill” kinetic non-nuclear interception and towards the use of other exotic technologies such as lasers and directed energy weapons.[[31]](#endnote-31) In the past two decades, enormous advances in computing, sensor and processing power have theoretically made kinetic and non-nuclear interception more feasible. At the same time, interest in BMD has spread beyond the United States and Russia, and systems are currently being developed and deployed by all major nuclear armed states.[[32]](#endnote-32)

Right of launch BMD relies on a number of essential technologies, sophisticated computers, processors, sensors and support systems in order detect missile launches, track the missile in flight, launch and guide interceptor missiles or other weapons to the target, and to do all of this in a matter of minutes. It is these technical challenges that have often been cited by those unconvinced about the efficacy of BMD, but the reality is that the performance varies between systems and depending on the nature of the threat and target being defended.[[33]](#endnote-33) The US Aegis system for example, often cited as amongst the most capable, successfully intercepted and destroyed an ICBM in November 2020.[[34]](#endnote-34)

Notwithstanding any debate about the technical efficacy of *right of launch* interception, the political impact has been significant. Russia and China have cited US missile defence plans as a key reason for nuclear modernisation, and particularly for the development of hypersonic missiles.[[35]](#endnote-35) Pakistan has similar concerns about Indian BMD plans. But the anxiety is not specifically about the capability of what has been deployed now but about what might follow, and how BMD might combine with other capabilities, particularly, precision strike.[[36]](#endnote-36) The worry is a future scenario where the US (or another state) might be able to conduct attacks, or at least threaten to destroy nuclear weapons while relying on a defence to soak up any retaliation. Of course, this also means that the extensive support apparatus that underpins BMD present potential targets for any would-be attacker (i.e., jam or destroy a radar or satellite to undermine the system) in the event of a crisis.

The idea of *left of launch* is to increase the overall efficacy of missile defence by seeking to prevent missiles from being fired, or at least to interfere with the launch process so that they can’t hit their intended targets.[[37]](#endnote-37) An example of this might be malware inserted into a missile or delivery platform that prevented the weapon from working. It could also involve electronic attacks against guidance systems or against other essential support apparatus so that the missile veers off-course or explodes. It is possible that the US has already attempted to undermine North Korea’s nuclear and missile programme in this way, although details unsurprisingly are scarce.[[38]](#endnote-38) Left of launch operations could also be undertaken using kinetic precision strike munitions (and maybe using hypersonic missiles as discussed above).[[39]](#endnote-39) When combined with right of launch capabilities, this creates what has been termed “full spectrum missile defence”.[[40]](#endnote-40)

Left of launch operations, especially using non-kinetic weapons, add an extra lay of complexity and potential instability to nuclear operations.[[41]](#endnote-41) First, left of launch attacks, especially CNOs, will probably rely on breaking into systems before they are used. This not only effectively moves the BMD mission from one of defence to pre-emption, but also raises the risks that the malware is discovered and leads to a crisis. Second, attempting to infiltrate the computer systems used for nuclear and missile command and control runs the risk of accidentally causing something to happen which wasn’t intended, such as infiltrating or impacting different systems. This is especially concerning for weapons held at high levels of alert, or if such actions were to be discovered during a crisis and interpreted as a pre-emptive attack. Third, the intangible nature of CNOs (especially when compared to the very palpable nature of right of launch BMD radar and interceptors) could drive greater fear and uncertainty. The capability of right of launch BMD can be roughly ascertained, incorporated into planning, and perhaps countered or overcome accordingly. But this will be much more difficult for left of launch, where it will be virtually impossible to ascertain who the capability is designed to be used against and how powerful/capable it is. Fourth, left of launch may be interpreted as a means to conduct disarming, counterforce attacks against nuclear weapons, or at least to threaten this in order to coerce.

Ballistic missile defence is not new (the pursuit of such capabilities can be traced back to the 1940s and attempts to protect against the Nazi V-weapons), and neither are concerns about its potentially destabilising impact. However, more capable and diverse interception capabilities combined with pre-emptive left of launch operations could make BMD more credible against a broader range of missile threats. The US has already been fairly explicit that it sees the integration of these capabilities as key to future planning, and it is likely that others will follow suit. The impact is likely to be not only disruptive, but also potentially highly destabilising.

**Complexity and escalation pathways across different domains**

The global nuclear ecosystem can be thought of as the broader contextual environment within which nuclear decisions, operations and thinking takes place. It is made up of hard, physical, and material components, such as weapons systems and targets, as well as softer, less tangible dynamics such as the way that nuclear-related information is signalled, gleaned, interpreted, used or interfered with. Both play a co-constitutive role in shaping nuclear order and the nature of nuclear risks. In addition to the complexity produced by the dynamics discussed above, two further developments are worth unpacking. The first is the concern that a greater reliance on space assets and concurrent developments in counter-space weaponry could lead to escalation. The second, is the more incorporeal challenge posed by a real-time, democratised and porous global nuclear information environment. The fear is that both open up new pathways to escalation and possibly nuclear use.

Modern military’s, especially in the United States, are increasingly reliant on “space” (that is the domain on the other side of the “Karman Line”, approximately 100km above the Earth’s surface). While most uses of space are designed to support conventional military missions, space assets also play a role in nuclear operations: missile launch detection and early warning, satellites to track incoming missiles or aircraft and to guide precision munitions (including nuclear-armed cruise or hypersonic missiles), as well as broader situational awareness. But this increasing dependence has created two interlinked concerns: First, that satellites might be targeted early in a crisis by an adversary, which makes targeting and destroying ASAT capabilities a priority, which in turn could drive escalation; and second, that attacks on space assets may be misinterpreted or that operations interrupt different systems from those intended, possibly because some satellites have dual functions. This is part of what James Acton has warned of as the entanglement problem, that attacks on nuclear command, control and communications assets based in space could be dangerously misinterpreted.[[42]](#endnote-42)

ASAT isn’t new[[43]](#endnote-43), but the ability to conduct non-nuclear counter-space operations, either through direct ascent and co-orbital weapons or by using other means (such as directed energy weapons) is.[[44]](#endnote-44) All major nuclear-armed states are engaged in ASAT development, and some have already demonstrated this capability.[[45]](#endnote-45) In 2007, a Chinese ASAT weapon destroyed a weather satellite at an altitude of 850km; the US destroyed a reconnaissance satellite at an altitude of 250km in 2008,[[46]](#endnote-46) and in 2019 India destroyed a satellite at an altitude of 282km.[[47]](#endnote-47) It is unlikely that a state could carry out a “perfect storm” and destroy all space assets in one go (satellites can be repurposed, some are a long way away and in different orbits, and a lot of different weapons would be required), but their vulnerability given their strategic importance and thus the potential for escalation is clear.

Space capabilities are part of a broader quest for information superiority and dominance, but this too is becoming more complex, in part due to the emergence of a new grey zone of conflict. Specifically, we are now living in a world of real-time information flows facilitated by information technology, social media platforms and global networks, where it is becoming more difficult to discern what is and isn’t true in a nuclear environment often characterised by too much rather than too little information.[[48]](#endnote-48) It is also a realm ripe for competition and mischief, which will have significant implications for managing nuclear risks.

There are a number of worrying dynamics that flow from this: First, this new environment complicates nuclear signalling. This could be because different entities are using different methods, e.g., through Twitter[[49]](#endnote-49), or because actions are interpreted incorrectly.[[50]](#endnote-50) The US Stratcom ill-conceived New Year’s Eve tweet about “dropping a bomb” might be an example of this.[[51]](#endnote-51) Second, unlike in the past, international events and actions that might preclude or exacerbate a nuclear crisis will be reported in real-time and be available publicly to all. This may make it difficult for leaders to take time to think through actions and increase the potential for an adversary to shape public opinion in a way that is detrimental. The classic example here is to think through how the Cuban Missile Crisis would have played out if it had happened today,[[52]](#endnote-52) or what impact the 2018 false missile alert in Hawaii might have had during a real nuclear crisis.[[53]](#endnote-53) Third, there is greater potential for “weaponised social media”, disinformation and misinformation, particularly from third party actions that might lead to what Rebecca Hersman has described as “wormhole escalation”.[[54]](#endnote-54) The use of deep fakes or other types of “fake news” could be used deliberately to deepen a crisis. We have already seen how fake news stories could lead to a nuclear warning when a bogus news story prompted Pakistan to issue a public warning Israel,[[55]](#endnote-55) and it should be assumed that sophisticated information operations will form part of any future nuclear crisis or conflict.[[56]](#endnote-56)

Modelling nuclear escalation has always been an art rather than a science[[57]](#endnote-57), but there is reason to believe that newly deployed disruptive technologies will make signalling, avoiding inadvertent escalation (especially from the conventional to nuclear domain), and controlling nuclear crisis more complicated. In particular, the commingling of conventional and nuclear support systems, especially in space, and a more blurred and global nuclear information ecosystem susceptible to interference, will open up new pathways to nuclear use and perhaps necessitate a change in how we mitigate nuclear risks.

**Understanding the AI-automation-nuclear nexus?[[58]](#endnote-58)**

Artificial Intelligence, and especially Automation already has a number of different applications across nuclear systems and have actually been around for decades. But there is undoubtedly potential for these technologies to play ever-greater roles in the future that could lead to increased instability and nuclear risks. The extent to which this might be seen as destabilising and hazardous depends on how such capabilities are deployed and what tasks they are assigned, and this in turn will be dependent upon the risk-reward calculations of military planners. There are good reasons why AI and Automation won’t become the ultimate destabilising development that some fear, but a certain degree of technological impetus, spill-over from applications in non-nuclear weapons systems, and perhaps a failure to think through the wider implications do present serious concerns.

AI is essentially coding, computer systems and software capable of performing tasks that require intelligence if carried out by humans. It is not one discrete system, but rather something than can be applied in many different ways depending on the particular task (this is why it makes little sense to talk of AI arms control). It is useful to distinguish between narrow AI, which has specific goals and is limited by its programming and the “problem” to be solved, and general AI that involves writing software that allows systems to “learn” through analysing datasets.[[59]](#endnote-59) The majority of what we term AI, and especially the systems currently used across the nuclear enterprise are rules-based narrow “if-then” types (principally because they are predictable), but the computer and information technology revolution mean that the requisite processing power and expertise has created the possibility for wider applications.[[60]](#endnote-60)

Autonomy/Automation is the application of AI to particular tasks, some of which might involve robotics, and therefore Automated or Autonomous weapons systems. There are different variations of Autonomy when it comes to weapons and support systems in terms of function and sophistication. These distinctions exist along a continuum from discrete *Automated* systems to more capable and goal-orientated *Autonomous* systems[[61]](#endnote-61)). Automation has been used for decades in in nuclear early warning, targeting and delivery systems (though most involve human control).[[62]](#endnote-62) AI essentially allows robotic systems to operate without human intervention, based on interaction with their environment, albeit to different extents.

Applications of AI, robotics and machine learning are theoretically endless and could be applied right across the nuclear enterprise. However, at the moment, applications of these technologies are limited by the huge datasets (and the security of data) required for training (especially for systems performing functions where there isn’t much data), the problem of control and unpredictability, computational power, and by a desire to keep humans “in the loop” (although this can be a double-edged sword due to automation bias and trust gaps).

AI and Autonomy are likely to play an important role in the software, computer and associated systems that support decision-making and nuclear command, control and communications.[[63]](#endnote-63) There is some precedent here: both the US and Russia built nuclear early warning systems during the Cold War that contained a degree of Automation (the so-called Dead Hand being a good example). But it is likely that AI and Autonomy could become increasingly important in data collection, data cleaning, and complex data analysis, for enhanced warning systems, targeting plans, and situational awareness. This may on the whole be a good thing: enhancing reliability and providing more time for decisionmakers in a nuclear crisis.[[64]](#endnote-64)

Another area of nuclear operations likely to benefit from AI and greater Autonomy is the ability to locate, track and target concealed and mobile nuclear systems. The combination of enhanced sensor capabilities across all domains (potentially deployed on semi or autonomous platforms or in “swarms”), the ability to transfer enormous caches of data quickly and analyse in real-time, and to deploy uninhabited systems to attack targets, may be changing the game of “nuclear hide and seek” (as discussed above).

AI and Automation could enhance guidance and accuracy of nuclear and conventional weapons systems by making missiles and bombs “smarter” and able to respond to their environment and change flight paths after being launched.[[65]](#endnote-65) A basic version of this type of AI is used in some cruise missiles and could be used in hypersonic missiles. If weapons can become more accurate it raises the possibility of surgical long-range counterforce strikes with conventional rather than nuclear weapons.

AI and Automation could facilitate the deployment of increasingly autonomous nuclear and non-nuclear delivery platforms. The best example is the Russian Status-6 nuclear-armed torpedo, but it is possible that other future nuclear delivery platforms could have a degree of autonomy (or at least be uninhabited).[[66]](#endnote-66) In the future, nuclear delivery platforms could be able to “loiter” stealthily near targets waiting to strike like the autonomous “Harpy” Uninhabited Aerial Vehicle (UAV) fielded by Israel.[[67]](#endnote-67) Though this would pose significant issues for command and control. Indeed, at the time of writing, the US military has publicly rejected the idea that the next generation strategic bomber (the B-21 Raider) will be unmanned for nuclear operations.

Other applications could include intelligent computer software able to defend nuclear networks or facilitate “left of launch” attacks on nuclear, missile and command and control systems.[[68]](#endnote-68) AI might also be used to create “Deep Fakes” for disinformation campaigns that might be used to precipitate or deepen a nuclear crisis.[[69]](#endnote-69)

All of these applications are potentially worrying, especially those that might undermine secure second-strike forces, complicate civilian command and control, or create new pressures and unforeseen pathways towards escalation. It is conceivable that advances in sensing and processing capabilities, perhaps deployed on autonomous platforms, combined with more accurate kinetic and digital weapons could be seen as a major threat to deterrence and stability, and drive arms racing. Military planners may become suspicious of this nuclear risk environment, not least due to the intangibility and ubiquity of the major driving technologies (in stark contrast to the weapons of the past). In a worst-case scenario, planners might become so concerned about the vulnerability of their nuclear forces that waiting to strike second may no longer be an option.

AI-enabled weapons systems are unlikely to be unopposed, and the software and programming that makes these weapons so capable may also prove to be their Achilles Heel. Any type of AI would be vulnerable to hacking, spoofing and data poisoning, and the risk would arguably increase the more sophisticated the capability became. Likewise, the Automated/Autonomous platforms used for sensing, communications and weapons delivery would be vulnerable to opposing forces, whether air defence against UAVs, jammers, cyber-attacks, or similar techniques underwater.[[70]](#endnote-70)

AI and Automation are not going away, and both are likely to play an ever-greater role in all aspects of nuclear operations going forward. However, so far nuclear-armed states have appeared determined to keep a “human in (or at least on) the loop” and are reluctant to delegate the most safety-critical nuclear operations to machines. The is due to a wariness of exactly how these systems might perform in real-world circumstances and a lack of understanding of more sophisticated systems would reach decisions.

This suggests that while arms control for certain specific applications of AI will be difficult (and the idea AI arms control in general a misunderstanding of the challenge) an agreement not to deploy fully Autonomous nuclear weapons without human control could be politically possible.[[71]](#endnote-71) But as the technical ability to do so increases, and if the nuclear order continues to deteriorate, we could see a move from specific applications of narrow AI in the nuclear realm to increasingly Autonomous weapons and support systems.

**Conclusion: Disruptive technology and the primacy of politics**

We are living through a period of significant technological flux in the nuclear space, where disruptive dynamics are impacting deterrence, proliferation, escalation, stability, and arms control. There is even a feeling that a certain technological determinism is driving us, wittingly or not, into a more dangerous nuclear order, where the risks of nuclear use are transformed and perhaps exacerbated. Unlike in the past, it is not just one technology or weapons system that is disrupting established thinking and frameworks, but a whole suite of systems and a concomitant transformation in the nuclear environment. When taken together these developments appear to blur the delineation between nuclear and non-nuclear weapons systems, create new pathways for (inadvertent escalation) through entanglement and indistinguishability, alter the perception of possible non-nuclear first-strike capabilities, increase the speed of operations and reduce decision-making time, generate greater uncertainty through a less tangible nature, and perhaps shift the balance between humans and machines. These risks are being compounded by what appears to be a lack of understanding by policymakers, a return to great power military competition, posturing and rhetoric, and at best a feeling that we are sleepwalking into this new era.

However, when thinking about this challenge it is important to consider why, how, when and to whom these different dynamics might be disruptive, and the differences between technologies. For example, *some* nuclear armed submarines and *some* mobile missiles *might* be becoming more vulnerable due to advances in tracking, targeting and precision strike, rather than all. Albeit the fear of this future possibility seems likely to drive modernisation and perhaps expansion and diversification of nuclear forces for all. Likewise, hypersonic weapons are not a counter-force game changer, but they do seem likely to increase the risks of misperception and inadvertent escalation. The key with hypersonic weapons will be keeping nuclear and non-nuclear systems separate and distinct in a viable way, and perhaps subject to arms control agreements. Of greater concern is the prospect that if left of launch and full-spectrum missile defence becomes normalised it will exacerbate considerably the current concerns over right of launch BMD. The emphasis is on the US as the leader in this field to prevent this from happening, especially as others may soon “catch up”. The potential applications of AI and Automation across the nuclear realm are considerable (including for sensing, tracking and targeting), but there are good reasons why this might be limited unilaterally, and perhaps multilaterally with the requisite political will. Political engagement will also be required to mitigate and manage the risks of a more complex global nuclear environment. It is essential that the escalation risks created by the deployment of new hard weapons systems and at the same time softer dynamics, are understood and factored into planning. Establishing secure lines of communication, clear signalling and understanding of an adversary’s different systems and processes is essential to prevent unwanted outcomes. In general, it seems that while non-nuclear weapons are not likely to supersede nuclear weapons soon (due to their enormous destructive power nothing else would have the same deterrent effect), increasingly capable non-nuclear and intangible weapons will play an ever more important role in nuclear politics, potentially creating different risks as we go forward.[[72]](#endnote-72)

While in no way wishing to downplay this challenge, there are reasons to be cautiously optimistic when it comes to the impact of disruptive technology on nuclear politics. The first is that the impact of disruptive technology isn’t new in the nuclear realm, and that periods of unsettling and rapid technological change have been managed in the past, and new mechanisms and frameworks developed accordingly. For sure, the challenge this time around appears to be more comprehensive and multifaceted, but just as new mechanisms were found to control the impact of “new technologies” in the past, we can do so again today. The second is that there has been tendency for hype and worst-case scenario thinking when it comes to the impact of various technologies on nuclear risk, but the reality is that the impact is often more nuanced and, in some cases, more marginal, or at least perceptual, than feared. This is sometimes because of a lack of understanding about the specifics of the challenges, or more often a failure to put the particular challenge or technological development in political and perhaps more importantly, budgetary context. The third is that the development of disruptive technologies, the thinking and doctrines that underpin them, and how they may impact nuclear relationships and order, are all fundamentally political dynamics. While technological drivers clearly are important in shaping nuclear order, this is a political problem that can have political solutions for risk reduction and the maintenance of stability. As such, while nuclear risk is changing, and we may well be moving into a new phase in the history of nuclear weapons, it should be possible to manage this transition and alter the frameworks of global nuclear governance accordingly.[[73]](#endnote-73)

1. Professor of International Politics, University of Leicester, UK. Ajf57@le.ac.uk. [↑](#endnote-ref-1)
2. For recent literature on this topic see: Christopher Chyba, “New technologies and strategic stability”, *Daedulus*, 149:2 (2020), pp.150-170; Todd S. Sechser, Neil Narang & Caitlin Talmadge, “Emerging technologies and strategic stability in peacetime, crisis, and war,” *Journal of Strategic Studies*, 42:6 (2019), pp.727-735. [↑](#endnote-ref-2)
3. E.g., Bernard Brodie, *Strategy in the missile age,* (Princeton University Press: 1959), and Robert Jervis, *The meaning of the nuclear revolution: Statecraft and the prospect of Armageddon* (Ithaca, N.Y.: Cornell University Press, 1989). [↑](#endnote-ref-3)
4. See for example, Colin Gray, *The second nuclear age,* (London, Lynne Rienner: 1999); Paul Bracken, *Fire in the East: The Rise of Asian Military Power and the Second Nuclear Age* (New York: Harper Collins, 1999); Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington, KY: University Press of Kentucky, 1996); Vipin Narang, *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict* (Princeton, N.J.: Princeton University Press, 2014). [↑](#endnote-ref-4)
5. For example, B.T. Feld, T. Greenwood, GW Rathjens, S Weinberg (eds), *Impact of new technologies on the arms race,* (London, The MIT Press: 1971), J.J. Gertler, *Emerging technologies in the strategic arena: A primer,* (RAND Corporation: March 1987) and Carl Builder, *Strategic conflict without nuclear weapons,* (RAND Corporation: April 1983). [↑](#endnote-ref-5)
6. Austin Long & Brendan Rittenhouse Green, “Stalking the secure second strike: Intelligence, counterforce and nuclear strategy”, *Journal of Strategic Studies,* 38:1-2 (2015), pp.38-73 [↑](#endnote-ref-6)
7. As Bryan Clark explains, “Since the Cold War, submarines—particularly quiet American ones—have been assumed to be largely immune to anti-access threats. Yet the ability of submarines to hide through quieting alone will decrease as each successive decibel of noise reduction becomes exponentially more expensive and new detection techniques mature that rely on phenomena other than the sounds emanating from a submarine. Bryan Clark, “The emerging era in undersea warfare”, *Center for Strategic and Budgetary Assessments,* (2015), p.8.

   Likewise, Paul Bracken has argued that, “The hunt for mobile missiles is getting faster, cheaper, and better.  Long recognized problems with mobile systems have combined with cyber technology breakthroughs to make these missiles vulnerable.” Paul Bracken, “Nuclear stability and the hunt for mobile missiles”, *Foreign Policy Research Institute,* (8 April 2016). See also, Paul Bracken, *The Hunt for Mobile Missiles: Nuclear Weapons, AI, and the New Arms Race*, (Philadelphia, PA: Foreign Policy Research Institute, 2020). [↑](#endnote-ref-7)
8. Computer Network Operations or CNO is a better descriptor than the more nebulous “cyber”. See, Andrew Futter, “Cyber semantics: Why we should retire the latest buzzword in security studies”, *Journal of Cyber Policy,* 3:2 (2018), pp.201-216. [↑](#endnote-ref-8)
9. Keir Lieber & Daryl Press, “The new era of counterforce: Technological change and the future of nuclear deterrence”, *International Security,* 41:4 (Spring 2017), pp.9-49. For a discussion see, Ryan Snyder & Benoit Pelopidas & Keir Lieber & Daryl Press, “Correspondence: New era or new error? Technology and the future of deterrence”, *International Security,* 43:3 (Winter 2018/2019), pp.190-193. [↑](#endnote-ref-9)
10. See, James R. Holmes, “Sea changes: The future of nuclear deterrence”, *Bulletin of the Atomic Scientists,* 72:4 (2016), pp.228-233. [↑](#endnote-ref-10)
11. Ballistic missiles deployed in silo’s are probably also becoming more vulnerable due to increases in accuracy. But this isn’t necessarily a new dynamic. [↑](#endnote-ref-11)
12. See foe example, Owen R Cote, “Invisible nuclear-armed submarines, or transparent oceans? Are ballistic missile submarines still the best deterrent for the United States?”, *Bulletin of the Atomic Scientists,* 75:1 (2019), pp.30-35. [↑](#endnote-ref-12)
13. John Gower, “Concerning SSBN vulnerability – recent papers”, *BASIC,* (10 June 2016); Jonathan Gates, “Is the SSBN deterrent vulnerable to autonomous drones?”, *The RUSI Journal,* 161:6 (2016), pp.28-35. [↑](#endnote-ref-13)
14. For a discussion of this, see Li Bin, “Tracking Chinese strategic mobile missiles”, *Science & Global Security,* 15 (2007), pp.1-30. [↑](#endnote-ref-14)
15. James Lacey, “Battle of the bastions”, *War on the Rocks,* (9 January 2020), <https://warontherocks.com/2020/01/battle-of-the-bastions/> [↑](#endnote-ref-15)
16. R. Jeffrey Smith, “Hypersonic missiles are unstoppable. And they’re starting a new global arms race.”, *The New York Times Magazine,* (29 June 2019). [↑](#endnote-ref-16)
17. For an overview see, Kelley M. Sayler, “Hypersonic weapons: Background and issues for Congress”, *Congressional Research Service,* (Updated 27 August 2020) and Richard H. Speier, George Nacouzi, Carrie A. Lee, Richard M. Moore, *Hypersonic missile nonproliferation: Hindering the spread of a new class of weapons,* (RAND Corporation, 2017). [↑](#endnote-ref-17)
18. Other systems include hypersonic gun-launched weapons. [↑](#endnote-ref-18)
19. Kelley M. Sayler, “Hypersonic weapons: Background and issues for Congress”, *Congressional Research Service,* (Updated 27 August 2020), pp.4-9. [↑](#endnote-ref-19)
20. Ibid., p.9. [↑](#endnote-ref-20)
21. See, Tong Zhao, “Conventional Challenges to Strategic Stability: Chinese Perceptions of Hypersonic Technology and the Security Dilemma,” *Carnegie-Tsinghua Center for Global Policy*, (23 July 2018). [↑](#endnote-ref-21)
22. Kelsey Davenport, “India tests hypersonic missile”, *Arms Control Today,* (October 2020). [↑](#endnote-ref-22)
23. See, Dean Wilkening, “Hypersonic weapons and strategic stability”, *Survival,* 61:5 (2019), pp.129-148; James M. Acton, “Hypersonic boost-glide weapons”, *Science & Global Security,* 23 (2015), pp.191-219. [↑](#endnote-ref-23)
24. For an excellent counter to this, see Ivan Oelrich, “Cool your jets: Some perspective on the hyping of hypersonic weapons”, *Bulletin of the Atomic Scientists,* 76:1 (2020), pp.37-45. [↑](#endnote-ref-24)
25. A MARV’d warhead might actually have better terminal phase manoeuvrability than a hypersonic warhead. See, Cameron L. Tracy & David Wright, “Modeling the performance of hypersonic boost-glide missiles”, *Science & Global Security,* (2021), p.24. [↑](#endnote-ref-25)
26. For an excellent primer on re-entry vehicle technology see Matthew Bunn, *Technology of ballistic missile reentry vehicles,* in Kosta Tsipis & Penny Janeway, *Review of US military research and development, 1984,* (Massachusetts Institute of Technology: 1984). [↑](#endnote-ref-26)
27. Hypersonic glide vehicles might also be vulnerable to air-borne directed energy weapons during their guiding phase, see Aaron Kennedy, Jacob Allen, Jonathan Balakumar, Mark Hutchings & Daniel Cook, “Hypersonic missile defence, stopping the unstoppable”, *UK Project on Nuclear Issues Papers,* (RUSI: 2020). [↑](#endnote-ref-27)
28. Andrew Reddie, “Hypersonic missiles: Why the new ‘arms race’ is going nowhere fast”, *Bulletin of the Atomic Scientists*, (January 2020). [↑](#endnote-ref-28)
29. Historically, there has been a fairly clear distinction between nuclear-armed delivery vehicles and those that are used to deliver non-nuclear payloads. For example, being specific about which submarines carry nuclear missiles or being clear where nuclear armed missiles are based (at least for the major powers). [↑](#endnote-ref-29)
30. Wilkening, “Hypersonic weapons and strategic stability”, p.145-146. [↑](#endnote-ref-30)
31. Henry "Trey" Obering, “Directed Energy Weapons are real…and disruptive”, *PRISM*, 8:3 (2019), pp.36-47. [↑](#endnote-ref-31)
32. Keir Giles, *Russian ballistic missile defense: Rhetoric and reality,* (Strategic Studies Institute, US Army War College: 2015); Bruce W. MacDonald and Charles D. Ferguson, “Chinese strategic missile defense: Will it happen, and what would it mean? *Arms Control Today,* (November 2015); Zafar Khan, “India’s ballistic Missile defense: Implications for South Asian deterrence stability”, *The Washington Quarterly,* 40:3 (2017), pp.187-202. [↑](#endnote-ref-32)
33. See Matt Korda & Hans Kristensen, “US ballistic missile defenses, 2019”, *Bulletin of the Atomic Scientists,* 75:6 (2019), pp.295-306. [↑](#endnote-ref-33)
34. “US successfully conducts SM-3 Block IIA intercept test against an Intercontinental Ballistic Missile target”, *Defense News,* (17 November 2020), <https://www.defense.gov/Newsroom/Releases/Release/Article/2417334/us-successfully-conducts-sm-3-block-iia-intercept-test-against-an-intercontinen/> [↑](#endnote-ref-34)
35. Current US systems are optimised for shooting down objects in low earth orbit (such as ballistic missiles) rather than in the upper atmosphere (hypersonics). However, missile defence against hypersonic missiles is doable, but intercepting missiles from different platforms and different directions could be difficult. See, Kyle Mizokami, “How do you stop a hypersonic weapon? DARPA is looking for the answer”, *Popular Mechanics,* (28 January 2020), <https://www.popularmechanics.com/military/weapons/a30679336/darpa-hypersonic-missile/> [↑](#endnote-ref-35)
36. For example, M. Taylor Fravel & Evan S. Medeiros, “China’s search for assured retaliation: The evolution of Chinese nuclear strategy and force structure”, *International Security,* 35:2 (2010), pp.48-87 [↑](#endnote-ref-36)
37. As former US Undersecretary for Defense, Brian McKeon explains, “[W]e need to develop a wider range of tools and that includes the efforts underway to address such threats before they are launched, or “left of launch.” The development of left-of-launch capabilities will provide U.S. decision-makers additional tools and opportunities to defeat missiles. This will in turn reduce the burden on our “right-of-launch” ballistic missile defense capabilities. Taken together, left-of-launch and right-of-launch will lead to more effective and resilient capabilities to defeat adversary ballistic missile threats.” Brian P. McKeon, Statement before the Senate Armed Services Subcommittee on Strategic Forces, April 13, 2016, <http://www.armed-services.senate.gov/imo/media/doc/McKeon_04-13-16.pdf>. [↑](#endnote-ref-37)
38. See for example, David E. Sanger & William J. Broad, “Trump inherits secret cyber war against North Korean missiles”, *The New York Times,* (4 March 2017). [↑](#endnote-ref-38)
39. Thomas Karako, “Missile defense and the nuclear posture review”, *Strategic Studies Quarterly,* 11:3 (2017), pp.48-64. See also, <https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/151204_full_spectrum_transcript.pdf> [↑](#endnote-ref-39)
40. See, Missile Defense Review, 2019, <https://www.defense.gov/Portals/1/Interactive/2018/11-2019-Missile-Defense-Review/The%202019%20MDR_Executive%20Summary.pdf>, p.viii. [↑](#endnote-ref-40)
41. For a discussion of this see, Andrew Futter, “The dangers of using cyberattacks to counter nuclear threats”, *Arms Control Today,* (July/August 2016). [↑](#endnote-ref-41)
42. James Acton, “Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war”, *International Security,* 43:1 (2018), pp.56-99. [↑](#endnote-ref-42)
43. Laura Grego, “A history of anti-satellite programs”, *Union of Concerned Scientists,* (January 2012), <https://www.ucsusa.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf> [↑](#endnote-ref-43)
44. For a discussion of this, see Todd Harrison, Kaitlyn Johnson & Thomas Roberts, “Space threat assessment 2018”, CSIS Aerospace Security Project, (April 2018). [↑](#endnote-ref-44)
45. Brian Weeden & Victoria Samson, “Global counterspace capabilities: An open assessment”, *Secure World Foundation,* (April 2020). [↑](#endnote-ref-45)
46. Gregory Kulacki & Jeffrey G. Lewis, “Understanding China's antisatellite test,” *The Nonproliferation Review*, 15:2, (2008), pp.335-347 [↑](#endnote-ref-46)
47. See Ashley Tellis, “India’s ASAT test: An incomplete success”, *Carnegie Endowment for International Peace,* (15 April 2019), <https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884> [↑](#endnote-ref-47)
48. See, Harold A. Trinkunas, Herbert Lin, Benjamin Loehrke, *Three tweets to midnight: Effects of the global information ecosystem on the risk of nuclear conflict,* (Hoover Institution Press: 2020). [↑](#endnote-ref-48)
49. Heather Williams & Alexi Drew, “Escalation by tweet: Managing the new nuclear diplomacy”, *Kings College London Centre for Science & Security Studies,* (July 2020). [↑](#endnote-ref-49)
50. This is a theme in Jeffrey Lewis’ book, *The 2020 Commission Report om the North Korean nuclear attacks against the United States: A speculative novel,* (London, HW Allen: 2018). [↑](#endnote-ref-50)
51. Matt Stevens & Thomas Gibbons-Neff, “Military deletes New Year’s Eve tweet saying it’s ‘ready to drop something’”, *The New York Times,* (31 December 2019). [↑](#endnote-ref-51)
52. Danielle Jablanski, Herbert S. Lin, and Harold A. Trinkunas, *Retweets to Midnight: Assessing the Effects of the Information Ecosystem on Crisis Decision Making between Nuclear Weapons States*, chapter in Harold A. Trinkunas, Herbert Lin, Benjamin Loehrke, *Three tweets to midnight: Effects of the global information ecosystem on the risk of nuclear conflict,* (Hoover Institution Press: 2020). [↑](#endnote-ref-52)
53. See, Kristyn Karl & Ashley Litle, “This is not a drill: Lessons from the false Hawaiian missile alert”, *Bulletin of the Atomic Scientists,* (10 January 2019), <https://thebulletin.org/2019/01/this-is-not-a-drill-lessons-from-the-false-hawaiian-missile-alert/> [↑](#endnote-ref-53)
54. See Rebecca Hersman, “Wormhole escalation in the new nuclear age”, *Texas National Security Review,* 3:3 (Autumn 2020). [↑](#endnote-ref-54)
55. Emma Graham-Harrison, “Fake news story prompts Pakistan to issue nuclear warning to Israel,” *The Guardian*, (25 December 2016), <https://www.theguardian.com/world/2016/dec/26/fake-news-story-prompts-pakistan-to-issue-nuclear-warning-to-israel> [↑](#endnote-ref-55)
56. Nautilus Institute, “Social media storms and nuclear early warning systems: A deep dive and speed scenarios workshop”, (8 January 2019), <http://nautilus.org/wp-content/uploads/2019/01/Social-Media-Nuclear-War-Synthesis-Report-Final-Jan8-2019.pdf> [↑](#endnote-ref-56)
57. Although for an excellent overview see, Barry Posen, *Inadvertent escalation: Conventional war and nuclear risk* (Ithaca, N.Y.: Cornell University Press, 1991. See also, Herman Kahn, *On escalation: Metaphors and scenarios,* (Transaction Publishers: 2009). [↑](#endnote-ref-57)
58. This section draws upon, Andrew Futter, “Artificial Intelligence, Autonomy and nuclear stability: Towards a more complex nuclear future”, *Valdai Policy Brief,* (October 2020). [↑](#endnote-ref-58)
59. Vincent Boulanin, *Artificial Intelligence: A primer,* in Vincent Boulanin (ed.), *The impact of Artificial Intelligence on strategic stability and nuclear risk,* Volume I: Euro-Atlantic Perspectives, (SIPRI: May 2019), pp.13-14. [↑](#endnote-ref-59)
60. Edward Geist & Andrew Lohn, “How might Artificial Intelligence affect the risk of nuclear war”, (RANDCorporation: 2018). [↑](#endnote-ref-60)
61. Paul Scharre, *Army of none: Autonomous weapons and the future of war,* (London, WW Norton Company Inc: 2018), pp.27-34. [↑](#endnote-ref-61)
62. Michael Horowitz, Paul Scharre & Alexander Valez-Green, “A stable nuclear future? The impact of autonomous systems and artificial intelligence”, (December 2019), p.7. [↑](#endnote-ref-62)
63. An interesting example of this is VYRAN–a computer programme designed to warn Soviet leaders if the US achieved the potential for a nuclear strike. Matt Field, “As the US, China and Russia build new nuclear weapons systems, how will AI be built in?” *Bulletin of the Atomic Scientists,* (20 December 2019). [↑](#endnote-ref-63)
64. Horowitz, Scharre & Valez-Green, “A stable nuclear future?” p.1. [↑](#endnote-ref-64)
65. Jonathan Roberts, Adam Tunbridge, Paul Neale, Jennifer Insley & Rebecca Desmond, “Human vs machine: The role of Artificial Intelligence in nuclear weapons systems”, in Luba Zatsepina & Tom Plant (Eds.), *The 2020 UK Project on Nuclear Issues Papers,* (RUSI: October 2020). [↑](#endnote-ref-65)
66. David Hambling, “The truth behind Russia’s apocalypse torpedo”, *Popular Mechanics,* (18 January 2019), <https://www.popularmechanics.com/military/weapons/a25953089/russia-apocalypse-torpedo-poseidon/> [↑](#endnote-ref-66)
67. Charlie Gao, “The ultimate weapon of war no one is talking about”, *The National Interest,* (25 January 2019), <https://nationalinterest.org/blog/buzz/ultimate-weapon-war-no-one-talking-about-42497> [↑](#endnote-ref-67)
68. James Johnson & Eleanor Krabill, “AI, cyberspace, and nuclear weapons”, *War on the Rocks,* (31 January 2020). [↑](#endnote-ref-68)
69. Jon Christian, “Experts fear face swapping tech could start an international showdown”, *The Future,* (1 Feb 2018), <https://theoutline.com/post/3179/deepfake-videos-are-freaking-experts-out?zd=3&zi=54fxjizh> [↑](#endnote-ref-69)
70. For a view on why the UK SSBN’s will remain protected see, Gower, “Concerning SSBN vulnerability”. [↑](#endnote-ref-70)
71. Matthijs Maas, “How viable is international arms control for military artificial intelligence? Three lessons from nuclear weapons”, *Contemporary Security Policy,* 30:3 (2019), pp.285-311. [↑](#endnote-ref-71)
72. See Andrew Futter & Benjamin Zala, “Strategic non-nuclear weapons and the onset of a Third Nuclear Age”, *European Journal of International Relations,* (Forthcoming: 2021). [↑](#endnote-ref-72)
73. For a discussion of this see, Michael T. Klare, “A strategy for reducing the escalatory dangers of emerging technologies”, *Arms Control Today,* (December 2020). [↑](#endnote-ref-73)