EU Non-Proliferation and Disarmament Consortium

Promoting the European network of independent non-proliferation and disarmament think tanks

NON-PROLIFERATION AND DISARMAMENT PAPERS

No. 73 March 2021

EXPLAINING THE NUCLEAR CHALLENGES POSED BY EMERGING AND DISRUPTIVE TECHNOLOGY: A PRIMER FOR EUROPEAN POLICYMAKERS AND PROFESSIONALS*

ANDREW FUTTER

I. INTRODUCTION

There is considerable interest from different audiences across Europe in the impact of 'new', 'emerging' and 'disruptive' technologies on nuclear security, strategy and order.[1] It is now unusual to participate in any academic or policy discussion about nuclear issues that does not make reference to the range of technologies that are undermining or might weaken the frameworks for managing nuclear risk. While reference to this challenge is pervasive, it is not always matched with the same level of understanding or appreciation of nuance. In fact, there is little agreement on what the terms 'emerging' and 'disruptive' refer to or on what is or is not new, as well as a tendency to conflate potential threats and to adopt worst-case scenario thinking. It is certainly true that the development and deployment of various technologies across and within the nuclear ecosystem pose a number of challenges to Europe, but any attempt to mitigate and manage new nuclear risks must start with a proper understanding of what these dynamics and associated dangers are.[2]

While there is little agreement on what constitutes a new, emerging or disruptive technology, the

[1] The challenges posed to the nuclear order by rapid technological advances are not new. See e.g. Feld, B. T. et al. (eds), *Impact of New Technologies on the Arms Race* (MIT Press: London, 1971); Gertler, J. J., *Emerging Technologies in the Strategic Arena: A Primer* (RAND Corporation: Santa Monica, CA, 1987); and Builder, C., *Strategic Conflict Without Nuclear Weapons* (RAND Corporation: Santa Monica, CA, 1983).

[2] For a helpful aid to understanding see Sauer, F. and Schörnig, N., 'Emerging technologies: Challenges for arms control', Peace Research Institute Frankfurt, Learning Unit 15, [n.d.].

* The contents of this paper benefited from research conducted as part of the 'Towards a Third Nuclear Age' project, funded by the European Research Council, grant number: 866155.

SUMMARY

This paper is a primer for those seeking to engage with current debates on nuclear risk in Europe. It demystifies and contextualizes the challenges posed by emerging and disruptive technologies in the nuclear realm. It looks in detail at five significant and potentially disruptive technological developments—hypersonic weapons, missile defence, artificial intelligence and automation, counterspace capabilities, and computer network operations (cyber)—to highlight often-overlooked nuances and explain how some of the challenges presented by these developments are more marginal, established and manageable than is sometimes portrayed. By emphasizing the primacy of politics over technology when it comes to meeting nuclear challenges, this paper also seeks to provide a basis for targeted risk reduction and arms control, as well as normative recommendations for policymakers and professionals working across Europe.

ABOUT THE AUTHOR

Andrew Futter (United Kingdom) is Professor of International Politics at the University of Leicester, UK. He has written widely on nuclear weapon issues and the impact of disruptive technology, including most recently the second edition of his textbook, *The Politics of Nuclear Weapons*, and the monograph, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. He is currently working on a European Research Council-funded project investigating the shift towards a 'third nuclear age'.

preference in this paper is to use the term 'emerging and disruptive' as this captures not only what is novel, but also those challenges that are more established but might have shifted in importance.[3] Therefore, the challenge posed by emerging and disruptive technologies comprises those weapons, support systems and subsystems that have been significantly improved or recently deployed—or could be rapidly developed in the near future—and that have the potential to change the way in which nuclear operations are conducted, and how nuclear order, command and control, stability, deterrence, arms control, escalation and crisis management function.[4] Some of these dynamics are more established than others, and some may have more marginal implications. But what makes this challenge particularly acute is the fact that it is playing out globally, and the technologies are interwoven, reaching maturity at the same time, and are intrinsically both dual use (having civilian and military applications) and dual capable (able to support nuclear and non-nuclear operations). It is therefore the cumulative and combined effects rather than any individual development that are significant. This in turn is reflective of how the broader nuclear environment is being shaped by the current information age.

This paper has three objectives: first, to demystify this shifting nuclear risk landscape, and place developments in political, historical and strategic context; second, to provide a primer for those seeking to engage with current debates on nuclear risks and emerging and disruptive technologies; and, third, to outline a set of realistic risk reduction, arms control and normative recommendations for policymakers and professionals working across Europe. Section II examines the significance of hypersonic missiles. Section III considers the impact of ballistic missile defence (BMD) on European stability. Section IV looks at the costs and benefits of artificial intelligence (AI) and automation in nuclear operations. Section V explains the escalatory potential of anti-satellite (ASAT) weapons and counterspace weaponry. Section VI unpacks the relationship between computer network operations (CNOs) and nuclear weapons.[5] Section VII provides a set of recommendations and conclusions.

II. THE SIGNIFICANCE OF HYPERSONIC MISSILES

A hypersonic missile is a weapon that can travel at speeds above Mach 5 (five times the speed of sound, or 6174 kilometres per hour) while carrying a warhead that can be manoeuvred during flight, and be terminally guided towards its target. Unlike ballistic missiles, which follow a parabolic trajectory, hypersonic weapons glide or fly at a relatively constant height, which has the potential to reduce warning times and make them harder to detect. In theory, this combination of speed, accuracy, surprise and manoeuvrability makes hypersonic weapons more difficult to defend against than standard ballistic or cruise missiles, and therefore makes them more destabilizing. However, the reality is more nuanced.

Hypersonic, ballistic and cruise missiles

Two types of hypersonic weapon are currently being developed: hypersonic glide vehicles (HGVs) and hypersonic cruise missiles (HCMs).[6] HGVs use a rocket in the same way as a ballistic missile to launch a payload into the atmosphere. (This could be from air, land or sea.) Rather than continue on a curved trajectory into space and then back towards the target, however, HGVs skim across the upper atmosphere at an altitude of roughly 30 km, before descending to their targets. It might take longer for a state that does not possess space-based detection capabilities (and therefore relies on ground-based radar for early warning) to detect an HGV than a ballistic missile, and the flight time to the target could be shorter because of the

[3] For more recent literature see e.g. Chyba, C., 'New technologies and strategic stability', *Daedalus*, vol. 149, no. 2 (Spring 2020), pp. 150–70; Sechser, S., Narang, N. and Talmadge, C., 'Emerging technologies and strategic stability in peacetime, crisis, and war', *Journal of Strategic Studies*, vol. 42, no. 6 (2019), pp. 727–35; Futter, A. and Zala, B., 'Strategic non-nuclear weapons and the onset of a third nuclear age', *European Journal of International Security*, 11 Feb. 2021, pp. 1–21; and Bidwell, C. and McDonald, B., *Emerging Disruptive Technologies and their Potential Threat to Strategic Stability and National Security* (Federation of American Scientists: Washington, DC, Sep. 2018).

[4] This label could also include nanotechnology, quantum computing and 3D printing. See e.g. Biercuk, M. and Fontaine, R., 'The leap into quantum technology: A primer for national security professionals', War on the Rocks, 17 Nov. 2017; Gsponer, A., 'From the lab to the battlefield: Nanotechnology and fourth generation nuclear weapons', *Disarmament Diplomacy*, no. 67 (Oct.–Nov. 2002); and Kelley, R., 'Is three-dimensional (3D) printing a nuclear proliferation tool?', EU Non-Proliferation and Disarmament Consortium, Non-Proliferation and Disarmament Paper no. 54 (Feb. 2017).

[5] CNO is used instead of 'cyber'. See e.g. Futter, A., '"Cyber" semantics: Why we should retire the latest buzzword in security studies', *Journal of Cyber Policy*, vol. 2, no. 2 (2018), pp. 201–216.

[6] HGVs are also sometimes known as hypersonic *boost*-glide vehicles.

different trajectory. Notwithstanding the significant amount of heat that HGVs produce, which theoretically makes them easier to track with infrared sensors, their manoeuvrability and less predictable flightpaths could also make them better at evading some missile defences. The Russian Avangard and the Chinese DF-ZF, both of which purportedly entered service in 2019, and the now defunct US Falcon Hypersonic Technology Vehicle 2 are all examples of HGVs.[7]

However, the transformative nature of HGVs should not be overstated. Many ballistic missiles already travel at hypersonic speeds.[8] It is possible to 'steer' ballistic missiles, giving them some limited ability to change course, or to deploy manoeuvrable re-entry vehicles (MARVs).[9] While ballistic missiles are predominantly guided by astro-inertial mechanisms, rather than a global navigation satellite system, they can be terminally guided to increase their accuracy.[10] In addition, because HGVs slow down as they descend towards their targets (and while manoeuvring), they may be more susceptible to interception by certain terminal missile defences (see below) than ballistic warheads. HGVs and ballistic missiles are therefore better conceptualized as existing along a continuum and sharing many similarities.

Although they are capable of travelling at similar speeds to HGVs, HCMs are different from HGVs because they are powered by air-breathing scramjet engines and stay inside the earth's atmosphere. HCMs are unmanned aircraft that rely on a mixture of onboard and external guidance systems, which provides for great accuracy and manoeuvrability. They are much quicker than standard supersonic cruise missiles but travel at higher altitudes (around 20 km) where the air is thinner, making them theoretically easier to track than cruise missiles that hug the ground. HCMs are more likely to be used against targets at shorter ranges, in part due to the power and fuel requirements of the engines, but a large HCM could have a longer range. That said, scramjet technology poses considerable technical challenges and has been likened to 'keeping a match alight in a hurricane'.[11] Examples of HCMs include the US X51-A WaveRider, the Russian–Indian BrahMos-II and the Russian 3M22 Zircon.[12]

Implications of hypersonic weapons for strategic stability

Three implications of HGVs and HCMs are often cited as key challenges to nuclear stability. First, that they can be *nuclear-armed* and used to bypass an adversary's missile defence systems. In some cases, therefore they might be seen as strengthening deterrence. Second, that they can be used for long-range *non-nuclear* precision strikes, which could make it possible to undertake disarming attacks against nuclear forces, thereby undermining stability and deterrence.[13] A third, more indirect, implication is that the use of dual-capable hypersonic weapons for tactical missions or to prevent an adversary from gaining access to or using a certain geographical area (anti-access area denial operations) could lead to escalation.

The sophisticated guidance systems and high level of accuracy of hypersonic weapons make them potentially suitable for non-nuclear precision strike operations.[14] Previously, a large nuclear blast was needed to destroy small, hardened or mobile targets because the circular error probable (CEP) was relatively large.[15] Today,

[7] See e.g. Sayler, K., *Hypersonic Weapons: Background and Issues for Congress*, Congressional Research Service (CRS), Report for Congress R45811 (US Congress, CRS: Washington, DC, updated 27 Aug. 2020); and Malik, T., 'Death of DARPA's superfast hypersonic glider explained', Space.com, 23 Apr. 2012.

[8] The US Minuteman III or the Russian RS-28 Sarmat could reach speeds in excess of Mach 15.

[9] MARVs can provide similar benefits to hypersonic missiles. See e.g. Caston, L. et al., *The Future of the US Intercontinental Ballistic Missile Force* (RAND Corporation: Santa Monica, CA, 2014), pp. 67–73. For a helpful discussion of re-entry vehicles see Bunn, M., 'Technology of ballistic missile reentry vehicles', eds K. Tsipis and P. Janeway, *Review of US Military Research and Development, 1984* (Massachusetts Institute of Technology: Cambridge, MA, 1984).

[10] Astro-inertial mechanisms use the position of stars based on where the missile was launched from. Ballistic warheads can be terminally guided, but this depends on the speed at which they are travelling. See e.g. Oelrich, I., 'Cool your jets: Some perspective on the hyping of hypersonic weapons', *Bulletin of the Atomic Scientists*, vol. 76, no. 1 (2020), p. 42.

[11] Creech, G., 'Match in a hurricane: NASA's X-43A storms into hypersonic realm', NASA, 2 Feb. 2004.

[12] Speier, R. H. et al., *Hypersonic Missile Nonproliferation: Hindering the Spread of a New Class of Weapons* (RAND Corporation: Santa Monica, CA, 2017), appendix.

[13] Most current precision-strike munitions are launched in-theatre by ships, bombers or ground forces.

[14] Acton, J., *Silver Bullet: Asking the Right Questions about Conventional Prompt Global Strike* (Carnegie Endowment for International Peace: Washington, DC, 2013).

[15] The CEP is the measure of precision for weapon systems: the higher the number, the less precise the weapon. It is defined as the radius of the circle that covers the area around a target where the probability of impact of the projectile is 50%. See e.g. MacKenzie, D., *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance* (MIT Press: London, 1990).

however, such operations might be achieved using highly accurate non-nuclear warheads. Being able to conduct surgical strikes against the nuclear weapon systems that an adversary relies on for deterrence (a secure second strike) without using nuclear weapons could lead to instability if that state believed its nuclear forces were vulnerable to attack, and that non-nuclear weapons might be more 'useable' than nuclear weapons. An associated risk comes from the indistinguishability of hypersonic weapons. During a crisis, it would not be clear whether warheads were nuclear-armed or conventionally armed and, until very late, what the intended target was. That said, these issues are not new and also apply to ballistic missiles.

Hypersonic missiles are part of a broader concern that Keir Lieber and Daryl Press have termed 'a new era of counterforce'.[16] The idea is that delivery systems have become so accurate and sensors so good at locating and tracking targets that protecting and concealing weapon systems has become increasingly difficult.[17] The result is that nuclear forces that have long been seen as survivable and essential to nuclear deterrence might have become more vulnerable, although the situation differs for different actors.[18]

Limitations and recommendations

There are formidable technical barriers to deploying HGVs and HCMs. These include how to manage the heat produced by atmospheric resistance, how to maintain control of the warhead during flight and how to overcome countermeasures such as signal jamming.[19] There is also some debate about how much extra capability HGVs or HCMs provide over advanced ballistic and cruise missiles, which can already evade defences (especially if deployed on depressed trajectories that might also reduce flight times), manoeuvre and strike targets with a high degree of accuracy.[20]

Possible limitations notwithstanding, there is a recognition that hypersonic weapons need to be brought into existing arms control frameworks or that new mechanisms to reduce the potential risks that they pose need to be developed.[21] Dual-capable HGVs that use ballistic missile launchers or nuclear HCMs deployed on bombers could be counted under existing agreements such as the 2010 Treaty on Measures for the Further Reduction and Limitation of Strategic Offensive Arms (New START) between Russia and the United States.[22] New or separate agreements might be needed, however, for hypersonic weapons that are deployed in different ways, such as forward based on land or at sea, or by actors currently outside of formal arms control mechanisms. There is also a clear need for agreements that seek to address the risks posed to successful crisis management. The European Parliament recommendation to the postponed 2020 Review Conference of the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (Non-Proliferation Treaty, NPT) has already made this point.[23]

A number of European states and the European Union (EU) are already engaged in hypersonic research, albeit not for use on nuclear weapons.[24] This could therefore be an area in which Europe could lead on arms control discussions. European leaders and professionals should encourage Russia and the USA to continue to work towards bilateral limits and reductions of deployed nuclear weapons and strategic launchers and push for the inclusion of hypersonic weapons in any future agreements.[25] This might also involve broader measures to (*a*) keep nuclear and conventional hypersonic weapons separate, (*b*) delineate strategic and tactical applications where possible, (*c*) seek to prohibit deployment in Europe in an echo of the now defunct 1987 Treaty on the Elimination

[16] Lieber, K. and Press, D., 'The new era of counterforce: Technological change and the future of nuclear deterrence', *International Security*, vol. 41, no. 4 (Spring 2017), pp. 9–49.

[17] Bracken, P., *The Hunt for Mobile Missiles: Nuclear Weapons, AI, and the New Arms Race* (Foreign Policy Research Institute: Philadelphia, PA, 2020).

[18] For a discussion see Snyder, R. et al., 'Correspondence: New era or new error? Technology and the future of deterrence', *International Security*, vol. 43, no. 3 (Winter 2018/2019), pp. 190–93.

[19] One way of managing the heat produced might be by using nanotechnology. See e.g. Tucker, P., 'Nanotechnology is shaping the hypersonics race', *Defense One*, 19 Nov. 2019.

[20] Oelrich (note 10).

[21] Williams, H., 'Asymmetric arms control and strategic stability: Scenarios for limiting hypersonic glide vehicles', *Journal of Strategic Studies*, vol. 42, no. 6 (2019), pp. 789–813.

[22] Acton (note 14), p. 35.

[23] European Parliament, Report on a European Parliament recommendation to the Council and the Vice-President of the Commission/High Representative of the Union for Foreign Affairs and Security Policy concerning the preparation of the 2020 Non-Proliferation of Nuclear Weapons Treaty (NPT) review process, nuclear arms control and nuclear disarmament options, 2020/2004(INI), 25 Feb. 2020.

[24] Speier (note 12).

[25] Vaddi, P. and Acton, J. M., *A ReSTART for US-Russian Nuclear Arms Control: Enhancing Security through Cooperation* (Carnegie Endowment for International Peace: Washington, DC, 2020).

of Intermediate-Range and Shorter-Range Missiles (INF Treaty), and (*d*) perhaps sketch out a hypersonic weapons limitation and inspection agreement for all states developing this technology.[26] Interested policymakers and professionals across Europe should also work to include hypersonic weapons as part of broader nuclear security and export control discussions, including in the Missile Technology Control Regime and the Hague Code of Conduct against Ballistic Missile Proliferation.[27]

III. BALLISTIC MISSILE DEFENCE AND NUCLEAR STABILITY IN EUROPE

BMD is not a new technology—the idea has been around since the 1940s and systems have been deployed in the past—and questions remain about the technical efficacy of certain systems, especially against sophisticated threats.[28] However, improvements in sensing, tracking and processing capabilities, and in non-nuclear interception methods, as well as a broader political normalization, mean that BMD is playing an increasingly important role in global security.[29] The result is that BMD is becoming an established component of deterrence and assurance thinking in a way that is politically very different from the pursuit of BMD during the cold war, and especially the US Strategic Defense Initiative (SDI) of the 1980s.[30] The impact is being felt acutely in Europe, where BMD—and the deployment of both US and North Atlantic Treaty Organization (NATO) BMD systems in the region—plays an important role in regional security but is also a source of instability in European relations with Russia and is a possible spoiler in future arms control negotiations.

Background on ballistic missile defence

BMD is not a single system but a catch-all term that covers a multitude of different capabilities and support apparatus designed to defend different targets against different ballistic missile threats in different ways. Accordingly, some systems might be considered more destabilizing than others.

The most important distinction is between strategic or national BMD and tactical, theatre or battlefield BMD, although the difference between the two is blurred. National defences are designed to protect entire countries and their populations and have historically been seen as destabilizing. The Treaty on the Limitation of Anti-Ballistic Missile Systems (ABM Treaty), which was in force between 1972 and 2002 (when the USA abrogated the agreement), placed strict limits on US and Russian national BMD systems as this was seen as a way of managing the nuclear arms race. The logic was that, by limiting defences, stability might be achieved through mutual vulnerability.[31] At the other end of the spectrum are systems—such as the US Patriot, which was used in both Gulf wars—that seek to protect a small area against shorter-range missile threats. Such battlefield defences do not affect strategic stability. Slightly more problematic are BMD systems that straddle this gap, such as the US Aegis, as some deployments and some interceptors might be able to play a role in national missile defence.[32]

A ballistic missile has three stages of flight: (*a*) the boost/ascent phase, between launch and exiting the atmosphere; (*b*) mid-course, as the separated warhead (or warheads) travels through space; and (*c*) terminal, as the warhead (or warheads) re-enters the atmosphere and descends towards its target. Each phase offers opportunities for interception but also presents different challenges. The boost phase is the easiest for interception (including for HGVs) because the missile's trajectory is clear and it is travelling relatively slowly, but the interception requires quick reactions and, in

[26] United Nations Office for Disarmament Affairs, United Nations Institute for Disarmament Research, *Hypersonic Weapons: A Challenge and Opportunity for Strategic Arms Control: A Study Prepared on the Recommendation of the Secretary-General's Advisory Board on Disarmament Matters* (United Nations: New York, 2019).

[27] For further detail on the Missile Technology Control Regime (MTCR) and the Hague Code of Conduct against Ballistic Missile Proliferation (HCOC) see their respective websites.

[28] For interception at least, the sensor and weapon technologies developed for BMD are useful in other contexts.

[29] See e.g. McArdle Kelleher, C. and Dombrowski, P. (eds), *Regional Missile Defense from a Global Perspective* (Stanford University Press: Stanford, CA, 2015).

[30] Although some of the technologies developed as part of the SDI live on.

[31] The ABM Treaty did not ban deployment entirely. Each side was initially allowed to protect two sites with 100 interceptors. This was later reduced to one site. The US Safeguard system designed to protect an intercontinental ballistic missile field became operational in 1975 but was closed shortly afterwards. The Soviet BMD system protecting Moscow remains operational today. Burns, R. and Brune, L., *The Quest for Missile Defenses, 1944–2003* (Regina Books: Claremont, CA, 2003); and Gruntman, M., *Intercept 1961: The Birth of Soviet Missile Defense* (American Institute of Aeronautics and Astronautics: Reston, VA, 2015).

[32] Panda, A., 'A new US missile defense test may have increased the risk of nuclear war', Carnegie Endowment for International Peace, 19 Nov. 2020.

most cases, close proximity to the launch site. Mid-course interception is difficult because the separated warhead (or warheads)—possibly including decoys and other countermeasures—is travelling through space at thousands of kilometres per hour. (Interception is even harder with manoeuvrable warheads such as HGVs during this phase of flight.) Interception at the terminal phase is difficult because individual targets must be protected and there is the problem of debris if the warhead is destroyed close to the ground.[33] In general, the earlier in its flight the missile/warhead can be intercepted, the larger the area that can theoretically be protected and the more effective against missiles with multiple warheads or countermeasures a system would be.

Historically, BMD systems have relied on a nuclear or non-nuclear blast to intercept an incoming warhead in the mid-course or terminal phase of flight. More recently, systems have utilized non-nuclear kinetic 'hit-to-kill' intercept technologies. This is in part due to significant advances in support systems: the ability to detect missile launches with satellites, track warheads with radar and process information to facilitate interception capabilities plays a fundamental role in BMD. Work has also continued on capabilities that might be used in the boost phase, incorporating for example fast and reusable directed energy weapons (DEWs), such as a laser deployed on platforms on land, at sea or in space, or even electromagnetic railguns.[34] DEWs use concentrated energy rather than kinetic interception to interfere with or destroy targets.[35] DEW interception might also be the best option for countering HGVs.[36] A final possibility is a 'left of launch' operation that seeks to prevent missiles from being fired successfully, as opposed to 'right of launch', which involves interception after launch (see below).

The growth of ballistic missile defence in Europe

Notwithstanding certain support facilities located in the region, such as the Fylingdales early warning radar in the United Kingdom, for many years BMD was something that only indirectly affected Europe as a result of the ongoing programme in the USA and the impact that this was perceived to have on strategic stability and arms control with Russia.[37]

In the past decade, however, the USA, NATO and certain European states have begun to develop and deploy BMD systems in Europe. This can be traced back to the US 'Third Site plan' of 2007, whereby long-range interceptors would be deployed in Eastern Europe to counter possible ballistic missile threats from Iran.[38] This would later be replaced by the Phased Adaptive Approach implemented by the administration of President Barack Obama, which proposed to link future BMD deployments in Europe to specific threats from the Middle East.[39] At the time of writing, this system comprises a radar in Turkey, Aegis Ashore BMD systems in Romania and Poland, and Aegis ships in the Mediterranean. NATO, meanwhile, has moved to adopt BMD as part of its core mission, and NATO's Active Layered Theatre Ballistic Missile Defence (ALTBMD) involves contributions from a number of European NATO members.[40] While ALTBMD is principally about harmonizing and coordinating missile defence capabilities across NATO, the system is becoming increasingly interconnected with components of the US BMD system both in Europe and globally.[41]

There are both political and military drivers behind the development of BMD in Europe. Politically, US BMD deployments in Europe might help to strengthen NATO cohesion and ensure a US footprint in the region. Strategically, these assets could help to deter and defend against ballistic missile threats from

[33] Interception at the terminal phase is often described as endoatmospheric because interception occurs inside the atmosphere. Exoatmospheric refers to interception outside the atmosphere.

[34] Obering, H. T., 'Directed energy weapons are real … and disruptive', *PRISM*, vol. 8, no. 3 (2019), p. 39; and O'Rourke, R., *Navy Lasers, Railgun, and Gun-launched Guided Projectile: Background and Issues for Congress*, Congressional Research Service (CRS), Report for Congress R44175 (US Congress, CRS: Washington, DC, updated 2 Apr. 2020). Such capabilities might also be used for counterspace operations (see below).

[35] See e.g. Obering (note 34), pp. 36–47.

[36] Kennedy, A. et al., 'Hypersonic missile defence: Stopping the unstoppable', eds L. Zatsepina and T. Plant, *UK Project on Nuclear Issues Papers 2020* (Royal United Services Institute: London, 2020).

[37] It should also be noted that the missile defence system deployed to defend Moscow has always been part of the UK's nuclear deterrence calculations. See e.g. Baylis, J., 'British nuclear doctrine: The "Moscow Criterion" and the Polaris improvement programme', *Contemporary British History*, vol. 19, no. 1 (2005), pp. 53–65.

[38] Fitzpatrick, M., 'A prudent decision on missile defence', *Survival*, vol. 51, no. 6 (2009), pp. 5–12.

[39] See e.g. Sankaran, J., *The United States' European Phased Adaptive Approach Missile Defense System: Defending Against Iranian Missile Threats Without Diluting the Russian Deterrent* (RAND Corporation: Santa Monica, CA, 2020).

[40] NATO, 'Ballistic missile defence', updated 9 Oct. 2019.

[41] For an overview see US Department of Defense (USDOD), Office of the Secretary of Defense, *2019 Missile Defense Review* (USDOD: Arlington, VA, 2019).

the Middle East and help to coordinate capabilities between NATO members for battlefield operations. However, the problem has always been disentangling these perceived requirements from the deterrence and political relationship with Russia. Russia has long been concerned about US BMD plans and the possibility that its nuclear retaliatory capability could be undermined through comprehensive and integrated BMD deployments.[42] Indeed, Russia's development of hypersonic weapons is believed to be directly linked to the future challenges posed by BMD. Another part of the problem has been convincing Russia that the systems used for BMD and deployed in Europe could not be quickly repurposed to fire offensive intermediate-range weapons.

Concerns and possible limitations

The pursuit of BMD is not necessarily destabilizing, but leaders across Europe have several roles to play in reducing the possible risks of future BMD deployments. First, there needs to be a clear understanding of what different systems are able to do and the impact that certain deployments might have, particularly on Russia. Second, there needs to be a recognition in Europe that Russia is likely to view BMD unfavourably regardless of the system's technological capability. The spectre of the future matters as much as what is deployed now. Third, BMD deployments need to be seen in the broader context of regional arms control and any negotiations on the future of the approximately 200 US nuclear gravity bombs deployed at bases in Europe under the NATO nuclear-sharing agreement.[43]

These factors raise questions for leaders across Europe, but especially for the members of NATO, about plans for regional BMD, and whether future deployments of systems are worth the trade-off in terms of arms control and risk reduction measures with Russia. First and foremost, European members of NATO have an important role to play in ensuring that future deployments are shaped by specific threats and threat scenarios, and that both intentions and capabilities are as transparent as possible to Russia. While rekindling the ABM Treaty might be politically problematic, specific limitations in Europe may be possible, and this could be an area where the EU can play a role. Another option might be to revisit the idea of BMD cooperation with Russia in Europe. This could begin with data sharing but potentially evolve into something more concrete.[44] Either way, US/NATO missile defence plans in Europe cannot be delinked from the wider debates about the future of arms control and of US non-strategic nuclear weapons in Europe, and how best to maintain strategic stability and build confidence with Russia.

IV. ARTIFICIAL INTELLIGENCE AND AUTOMATION IN THE NUCLEAR REALM[45]

The apparent desire of a number of states to incorporate AI and automation into nuclear operations may seem alarming and may sometimes lead to comparisons with the apocalyptic plot lines from science fiction.[46] But while there are undoubtedly a number of concerns linked to the shifting balance between human and machine control in nuclear systems, it is not preordained that AI and automation will significantly increase nuclear risks or undermine strategic stability and nuclear security in Europe. Indeed, AI and automation have played a role in nuclear operations for many years and, if used properly, might even enhance security. The key will be to ensure that the possible dangers are understood by policymakers and to design appropriate risk reduction mechanisms accordingly.[47]

Artificial intelligence and automation: The basics

AI constitutes coding, computer systems and software capable of performing tasks that require intelligence if undertaken by humans. It is not one discrete system, but something that can be applied in many different ways depending on the particular task. 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 (not to

[42] See e.g. Ivanov, I., 'The missile-defense mistake: Undermining stability and the ABM Treaty', *Foreign Affairs*, vol. 79, no. 5 (2000), pp. 15–20.

[43] Futter, A., 'NATO, ballistic missile defence and the future of US tactical nuclear weapons in Europe', *European Security*, vol. 20, no. 4 (2011), pp. 547–62.

[44] See e.g. Blechman, B. and Vaicikonis, J., 'Unblocking the road to zero: US–Russia cooperation on missile defenses', *Bulletin of the Atomic Scientists*, vol. 66, no. 6 (2010), pp. 25–35.

[45] This section draws on Futter, A., 'Artificial intelligence, autonomy and nuclear stability: Towards a more complex nuclear future', Valdai Discussion Club, Expert Opinions, 15 Oct. 2020.

[46] Perhaps most notably, *The Terminator* (1984).

[47] See e.g. Boulanin, V. et al., *Artificial Intelligence, Strategic Stability and Nuclear Risk* (SIPRI: Stockholm, 2020).

be confused with artificial general intelligence—the notion of a super intelligence), which involves writing software that allows systems to 'learn' by analysing data sets and then to make decisions.[48] The majority of AI, and especially the systems currently used across the nuclear enterprise, are rules-based 'if-then' types, principally because they are predictable. However, the computing and information technology revolution has created the requisite processing power and expertise to allow for the possibility of wider applications.[49]

Autonomy/automation is the application of AI to particular tasks, some of which might involve robotics and therefore automated or autonomous weapon systems. There are different variants of autonomy in terms of function and sophistication. These distinctions exist along a continuum from discrete *automated* systems to more capable and goal-orientated *autonomous* systems.[50] AI essentially allows robotic machines to operate without human intervention based on interaction with their environment, albeit to different extents. Like AI, automation has been used in aspects of nuclear early warning, targeting and delivery systems for many decades, although most involve a high degree of human control.[51]

Applications in the nuclear realm

Looking forward, AI and autonomy could be used right across the nuclear realm. At present, however, greater integration is limited by the huge data sets needed for training (especially for systems performing functions where there is not much data), and the security of data required. There is also the problem of control and unpredictability, whereby the user may not be confident about how decisions were reached by using AI. Computational power and a desire to keep humans 'in the loop' also impose limits, although maintaining human oversight can be a double-edged sword due to automation bias, where human users are too willing to trust information produced by AI, and trust gaps, where users are reluctant to trust AI-produced information because the processes underpinning the generation of that information are not transparent.

AI and autonomy might play a role in the software, computer and associated systems that support decision making and nuclear command, control and communications (C3). There are precedents here: both Russia and the USA built nuclear early warning systems during the cold war that contained a degree of automation.[52] It is likely that AI and autonomy will become increasingly important in data collection, data cleaning and complex data analysis for enhanced warning systems, targeting plans and situational awareness. If this increases warning times, reliability and confidence (e.g. in missile early warning), it may prove beneficial for nuclear stability.

A second area of nuclear operations that may benefit from AI and greater autonomy is the ability to locate, track and target concealed and mobile nuclear systems. This is evolving through a combination of (*a*) enhanced sensor capabilities across all domains, potentially deployed on semi-autonomous or autonomous platforms or in 'swarms', (*b*) the ability to transfer enormous caches of data and analyse in real-time, and (*c*) the potential to deploy unstaffed systems to attack targets. Two possible applications stand out: the targeting of mobile, land-based nuclear missiles and the ability to locate nuclear-armed submarines.[53] At the same time, such capabilities might also help with verification for arms control.

A third potential impact might be on the guidance and accuracy of nuclear and conventional weapon systems. Improvements could be achieved by making missiles and bombs 'smarter' and able to respond to their environment after launch. A basic version of this type of AI is already being used in cruise missile guidance and could be used in hypersonic missiles.[54] If weapons can become more accurate, this raises the possibility of surgical long-range counterforce strikes using conventional rather than nuclear weapons (as discussed above).

[48] Boulanin, V., 'Artificial intelligence: A primer', ed. V. Boulanin, *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, vol. 1, *Euro-Atlantic Perspectives* (SIPRI: Stockholm, 2019), pp. 13–14.

[49] Geist, E. and Lohn, A., *How Might Artificial Intelligence Affect the Risk of Nuclear War?* (RAND Corporation: Santa Monica, CA, 2018).

[50] Scharre, P., *Army of None: Autonomous Weapons and the Future of War* (WW Norton: London, 2018), pp. 27–34.

[51] Horowitz, M., Scharre, P. and Valez-Green, A., 'A stable nuclear future? The impact of autonomous systems and artificial intelligence', arXiv.org, Dec. 2019.

[52] Most notably, the Russian 'dead hand'.

[53] Bracken (note 17). For background see Long, A. and Rittenhouse Green, B., 'Stalking the secure second strike: Intelligence, counterforce and nuclear strategy', *Journal of Strategic Studies*, vol. 38, nos 1–2 (2015), pp. 38–73. For a different view see Snyder, R. and Pelopidas, B., 'Correspondence: New era or new error? Technology and the future of deterrence', *International Security*, vol. 43, no. 4 (Winter 2018–19), pp. 190–93.

[54] Examples of cruise missile guidance of this type are Terrain Contour Matching (TERCOM) and Digitized Scene-Mapping Area Correlator (DSMAC).

Fourth, AI and automation could facilitate the deployment of increasingly autonomous nuclear and non-nuclear delivery platforms. A notable example is the Russian Status-6 nuclear-armed torpedo (known as Poseidon), but it is possible that other future nuclear delivery platforms could have a degree of autonomy, or be unstaffed.[55] Additionally, they may be able to 'loiter' stealthily near targets waiting to strike, in the same way as the autonomous Israeli Harpy unmanned aerial vehicle (UAV), although this would pose significant issues for command and control.[56]

Other applications might include computer software able to defend nuclear networks or facilitate left of launch attacks on nuclear, missile, and command and control systems.[57] AI might also be used to create deepfakes for disinformation campaigns that precipitate or worsen a nuclear crisis.[58]

All of these applications are potentially worrying, but especially those that might undermine secure second-strike forces or create new escalatory pressures and pathways. 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, drive arms races, and even increase the risk of nuclear use.

Managing risks and opportunities

AI-enabled weapon systems are unlikely to progress unopposed. The software and programming that make these weapons so capable may also prove to be their Achilles heel. AI would be vulnerable to hacking, spoofing and data poisoning, and the risk would probably increase as the system became more sophisticated. Similarly, the automated/autonomous platforms used for sensing, communications and weapon delivery would be vulnerable to opposing forces, be they air defence against UAVs, jammers, cyberattacks or similar techniques in other military domains.[59]

EU member states are already engaged at a number of different levels on the governance of AI and lethal autonomous weapon systems (LAWS), and some of them are playing a leading role in the push for regulation or ban of LAWS.[60] The EU is therefore perfectly placed to lead on specific recommendations for nuclear risk reduction in this space too.

First, European leaders and the EU should work towards a specific ban on the deployment of autonomous *nuclear* weapon systems, although this will probably require a very narrow definition to be technologically viable.[61] With the exception of Russia's Status-6 torpedo, the nuclear-armed states have so far appeared determined to keep a human in the loop and reluctant to delegate the most safety-critical nuclear operations to machines. This suggests that there may be some scope for an agreement of this type.

Second, professionals and academics working on this topic across Europe must educate policymakers on these technologies and the risks that they involve, so that the nature and seriousness of their application in the nuclear realm is understood at the highest levels. This would probably also involve engaging the private sector where many of the most important developments in AI and automation are taking place.

V. THE IMPORTANCE OF SPACE AND COUNTERSPACE WEAPONRY

Space has played a role in nuclear operations since the 1950s.[62] During the cold war, space became increasingly important for intelligence, surveillance and reconnaissance (ISR), nuclear early warning, and especially attempts to identify and locate nuclear facilities and launch sites. However, the opportunities and risks created by the interaction between space and nuclear operations are changing. This is partly because

[55] Hambling, D., 'The truth behind Russia's apocalypse torpedo', *Popular Mechanics*, 18 Jan. 2019.

[56] Gao, C., 'The ultimate weapon of war no one is talking about', *National Interest*, 25 Jan. 2019.

[57] Johnson, J. and Krabill, E., 'AI, cyberspace, and nuclear weapons', War on the Rocks, 31 Jan. 2020.

[58] Christian, J., 'Experts fear face swapping tech could start an international showdown: Video forensic specialists are worried deepfakes could have national security repercussions', *The Future*, 1 Feb. 2018.

[59] For a view on why British nuclear-powered ballistic missile submarines (SSBNs) will remain protected see Gower, J., 'Concerning SSBN vulnerability: Recent papers', British American Security Information Council Blog, 10 June 2016.

[60] European Parliament resolution of 12 Sep. 2018 on autonomous weapon systems, 2018/2752(RSP). See also Dahlmann, A., 'Towards a regulation of autonomous weapons: A task for the EU', European Leadership Network, 18 Jan. 2019.

[61] See e.g. Maas, M., 'How viable is international arms control for military artificial intelligence? Three lessons from nuclear weapons', *Contemporary Security Policy*, vol. 30, no. 3 (2019), pp. 285–311.

[62] Space is defined as the other side of the Karman Line, 100 km above the surface of the earth.

capabilities in space are becoming more important for nuclear and support operations and increasingly co-mingled with conventional military requirements. It is also a result of developments in non-nuclear and non-kinetic counterspace weapons.

What is space used for?

A multitude of assets deployed in different orbits around the earth play important roles in ISR, communications, nuclear early warning, and tracking, targeting and navigation.[63] While many nuclear weapons do not require satellites for guidance, some newer weapons (and possibly hypersonic missiles) as well as early warning and BMD do. Space assets will therefore represent an obvious target in future crises. There is a fear that this increases the risk of escalation, inadvertent or otherwise, which might lead to nuclear use. However, there are many different types of satellite with different functions and orbits, some of which are theoretically more vulnerable and escalation-prone than others.

There are different ways to classify satellites but perhaps the most useful is by the height of their orbit above the earth, as this affects their perceived vulnerability to ASAT weapons and what they are able to do.[64]

A number of satellites used for ISR (particularly those that require high resolution) are deployed in low earth orbit (LEO), between 100 km and 2000 km above the earth. Satellites in LEO circle the earth every 90–120 minutes but, due to their inclination, do not pass over the same spot every time. This means that multiple satellites are needed to maintain constant surveillance of a specific area. Satellites in this orbit might also be used for electronic intelligence (ELINT) or be fitted with thermal imaging, optical or infrared sensors for targeting. They can also use synthetic-aperture radar to create two-dimensional images or three-dimensional reconstructions of targets on the ground. Satellites in LEO are potentially useful for hunting mobile missiles. Piloted aircraft and UAVs have similar capabilities but are often restricted from an adversary's airspace.

Medium earth orbit (MEO), approximately 2000–24 000 km above the earth, contains satellites used for global navigation systems—which can be used to guide missiles and other munitions and to provide nuclear detonation detection—and some satellites used for ELINT.[65] Satellites at an altitude of 2000 km orbit the earth roughly every two hours while those at 24 000 km orbit roughly every 14 hours. With enough satellites in the upper part of this orbit (where navigation satellites are stationed), complete coverage of the earth can be achieved.[66] Such systems already play a role in cruise missile navigation and could be used to guide hypersonic or ballistic re-entry vehicles.

Satellites in geostationary orbit (GEO), approximately 35 800 km above the earth, orbit every 24 hours, meaning that they are able to remain over a particular area. This is also high enough that only a few are needed to monitor the entire planet. This orbit is used for satellite communications, for BMD, including the use of infrared sensors for missile launch detection (early warning), and for tracking hypersonic and ballistic warheads.

Counterspace threats and vulnerabilities

ASAT systems can be traced back to the 1950s and can involve kinetic interceptors (either direct ascent or orbital) deployed on rockets, rockets that deploy blast fragments or non-kinetic mechanisms such as lasers, jamming or hacking.[67] In theory, satellites in LEO are the most vulnerable because they are closest to the earth. A Chinese ASAT test destroyed a weather satellite at an altitude of 850 km in 2007 and the USA destroyed a reconnaissance satellite at 250 km in 2008.[68] In 2019 India destroyed a satellite at a height of 282 km.[69] It takes minutes to reach LEO using a direct-ascent weapon, but it takes several hours and a more

[63] The Union of Concerned Scientists lists 2666 satellites orbiting the earth, of which 330 are classified as being for military purposes. Others may be dual-use or able to be repurposed. Union of Concerned Scientists, Satellite Database, updated 1 Apr. 2020.

[64] For a comprehensive primer see British Ministry of Defence (MOD), *The UK Military Space Primer* (MOD, Development, Concepts and Doctrine Centre: London, June 2010).

[65] E.g. GPS (Global Positioning System), Galileo, GLONASS, COMPASS and BeiDou.

[66] GPS needs approximately 21 satellites for constant 3D positioning data.

[67] Grego, L., 'A history of anti-satellite programs', *Union of Concerned Scientists*, Jan. 2012. BMD and kinetic ASAT interception techniques are similar in LEO, albeit that there are differences in the 'hardness' of the target, time pressures and dealing with decoys.

[68] Kulacki, G. and Lewis, J. G., 'Understanding China's antisatellite test', *Nonproliferation Review*, vol. 15, no. 2 (2008), pp. 335–47.

[69] See e.g. Tellis, A., 'India's ASAT test: An incomplete success', Carnegie Endowment for International Peace, 15 Apr. 2019.

powerful booster to hit satellites in higher orbits. This of course would provide considerable warning time.

The vulnerability of satellites is not new but the ability to target satellites with non-nuclear and non-kinetic capabilities has become a major concern for those worried about escalation. This is partly due to the problem of dual-use space capabilities and how different attacks might be perceived.[70] One fear is that space and satellite capabilities might be attacked early in a crisis to prevent an opponent from being able to use them for ISR, BMD or precision strikes. Such attacks (and even pre-attack targeting) could be highly escalatory and possibly viewed as laying the foundations for a wider attack.[71] All the major nuclear powers are currently engaged in ASAT weapon development.[72] This raises the risk of inadvertent escalation in a future crisis, potentially from the conventional to the nuclear realm, although there is some scepticism about the viability of large-scale ASAT attacks.[73] Of course, satellites can be protected by deploying countermeasures or manoeuvring, or can even be equipped with offensive capabilities.[74] This, however, may require a bigger platform.

While the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (Outer Space Treaty) prohibits the placing of nuclear weapons or other weapons of mass destruction in space, this does not include lasers, or electronic or other non-nuclear kinetic weapons. A proposed Prevention of an Arms Race in Outer Space Treaty is still being discussed at the Conference on Disarmament (CD).[75]

Looking ahead: Europe, the EU and space

The EU and many EU member states already play an active role in the security and safety of outer space. While the draft EU proposal for an International Code of Conduct for Outer Space Activities is now effectively defunct, this should be seen as a start rather than the end of the process of seeking to manage the risks posed in this domain.[76] Indeed, given the emerging strategic picture and the risks posed by the entanglement of space and nuclear operations, there is a clear need to do more.

A good place to start would be to ensure that those in power understand the role of space in nuclear operations and stability, and how this reliance creates new escalation pathways. Where possible, this might involve seeking to disentangle commercial and military space assets and ensuring that policymakers across Europe are familiar with the different types of satellite, what they can do and how any aggressive actions against them might be perceived. The European Space Agency could have a role to play here, as would European states through the CD.

More challenging would be for European states and perhaps the EU to examine the possibility of restrictions or even a ban on direct-ascent ASAT weapons, or a moratorium on attacking certain satellites, such as nuclear early warning, that are central to stability. This would complement broader EU efforts on space risk reduction and arms control.

VI. NUCLEAR RISK AND COMPUTER NETWORK OPERATIONS

Computers have been a part of nuclear weapon systems from the start, and one of the first computers was developed specifically to assist with nuclear air defence in the 1950s.[77] As computing and processing power have increased, however, so too have the risks posed by the computer–nuclear weapons interface. Computers have facilitated improvements in nuclear safety and security, but a growing reliance on computer systems and networks has created new vulnerabilities that could be exploited.

The cyber–nuclear nexus

In the nuclear realm, the CNO/cyber challenge involves the risk of malicious actors interfering with the software, hardware, data, networks and processes

[70] Acton, J., 'Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war', *International Security*, vol. 43, no. 1 (2018), pp. 56–99.

[71] Morgan, F. E., *Deterrence and First-strike Stability in Space* (RAND Corporation: Santa Monica, CA, 2010).

[72] Weeden, B. and Samson, V., 'Global counterspace capabilities: An open assessment', Secure World Foundation, Apr. 2020.

[73] Sankaran, J., 'Limits of the Chinese anti-satellite threat to the United States', *Strategic Studies Quarterly* (Winter 2014), pp. 20–47.

[74] Obering (note 34), p. 41. See also Mizokami, K., 'We caught Russia testing a space-based weapon', *Popular Mechanics*, 23 July 2020.

[75] See e.g. National Threat Initiative, 'Proposed Prevention of an Arms Race in Space (PAROS) Treaty: Status', updated 23 Apr. 2020.

[76] European External Action Service, 'EU proposal for an international Space Code of Conduct, draft', 31 Mar. 2014.

[77] Redmond, K. C. and Smith, T. S., *From Whirlwind to Mitre: The R&D Story of the SAGE Air Defense Computer* (MIT Press: London, 2000).

of computer systems that govern weapons, command and control, communications and warning systems, as well the people and information that operate them.[78] Malicious interference may be intended to (*a*) prevent systems from working as they should, by stopping weapons from being used or undermining confidence in them, (*b*) enable a launch or explosion, or (*c*) exacerbate a nuclear crisis in some other way. Disabling attacks are more likely to be the preserve of nation state actors, while enabling attacks would appear more likely to be of interest to non-state actors. The vulnerability of a nuclear weapon system to hackers is a product of its reliance on digital software, the level of security and the extent to which it is separate from unsecured networks.

Any attacker wanting to compromise nuclear-related computer systems, data, networks and people could use a range of different vectors. The most difficult would be direct attacks on weapons and command and control apparatus, such as by gaining access to these highly protected networks in order to release malware into the system. Nuclear C3 systems will almost certainly be physically separated from outside networks, or 'air-gapped', but hackers have other ways in. It is thought, for instance, that Stuxnet managed to bridge an air-gap to attack the Iranian nuclear facility at Natanz.[79] The supply chain for hardware and software used across the nuclear enterprise might be targeted, although ensuring that the malware reaches the correct place would be difficult. Another option would be to interfere with the data and information needed by these systems, or with the human operators who rely on them, for instance, through social engineering or phishing attacks. Each of these challenges may be complicated by the 'attribution problem'—the fear that it will be difficult to identify at speed and with confidence who is responsible for such actions.[80]

Another challenge posed by the computer–nuclear weapons interface involves changes to the global nuclear ecosystem in which nuclear politics takes place. The risks here are driven by the real-time nature of global communications, by the democratization of participants (that is, the ability of more actors to access and influence global politics), and by a new type of nuclear information space that creates the possibility of misinformation or disinformation, for example, through Twitter.[81] One possible impact might be that stability during a crisis could be deliberately undermined at great speed and low cost.[82] All this has clear implications for signalling, crisis communications and inadvertent escalation between nuclear-armed opponents.

Left of launch operations

Perhaps the most acute concern in the cyber–nuclear space is the advent of left of launch operations. Left of launch is the use of CNO or other non-kinetic methods to prevent missiles from being fired, or at least to interfere with the launch process to prevent them from hitting their intended targets.[83] One example of this might be malware inserted into a missile or delivery platform that prevents a weapon from working. It could also involve attacks against guidance systems or against other essential support apparatus so that the missile veers off course or explodes. When combined with right of launch BMD capabilities (discussed above), left of launch operations add an extra layer of complexity and potential instability to nuclear operations.[84] This creates what has been termed 'full spectrum missile defence'.[85] There are a number of worrying aspects to this.

First, left of launch attacks will involve breaching systems before they are used. This effectively transforms the BMD mission from defence to pre-emption and increases the risk that the malware will be discovered and lead to a crisis.

Second, attempting to infiltrate the computer systems used for nuclear and missile command and control risks accidentally causing something to happen that is unintended, such as infiltrating or affecting different systems. This is especially concerning for

[78] See e.g. Futter, A., *Hacking the Bomb* (Georgetown University Press: Washington, DC, 2018). See also Unal, B. and Lewis, P., *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences* (Chatham House: London, 2018).

[79] Zetter, K., *Countdown to Zero Day: Stuxnet and the Launch of the World's First Cyber Weapon* (Crown Publishers: New York, 2014).

[80] See e.g. Rid, T. and Buchanan, B., 'Attributing cyber-attacks', *Journal of Strategic Studies*, vol. 38, nos 1–2 (2015), pp. 4–37.

[81] Williams, H. and Drew, A., *Escalation by Tweet: Managing the New Nuclear Diplomacy* (Kings College London, Centre for Science and Security Studies: London, July 2020).

[82] Trinkunas, H. A., Lin, H. and Loehrke, B., *Three Tweets to Midnight: Effects of the Global Information Ecosystem on the Risk of Nuclear Conflict* (Hoover Institution Press: Stanford, CA, 2020), pp. 9–10.

[83] See e.g. McKeon, B. P., Principal Deputy Undersecretary of Defense for Policy, Statement before the Armed Services Subcommittee on Strategic Forces, US Senate, 13 Apr. 2016.

[84] Futter, A., 'The dangers of using cyberattacks to counter nuclear threats', *Arms Control Today* (July–Aug. 2016).

[85] See e.g. US Department of Defense (note 41), p. viii.

weapons held at high levels of alert. Moreover, if such actions were discovered during a crisis, they might be interpreted as a pre-emptive attack.

Third, the intangible nature of CNOs could drive greater fear and uncertainty about the vulnerability and veracity of certain nuclear weapon systems. The capability of right of launch BMD can be roughly ascertained, incorporated into planning and perhaps countered or overcome. This would be much more difficult for left of launch BMD, however, where it is virtually impossible to ascertain who the capability is designed to be used against and how powerful or capable it is.

Fourth, left of launch could also be interpreted as a more practicable means of conducting disarming counterforce attacks against nuclear weapons when compared with kinetic attacks, or at least of threatening this in order to coerce.

The USA might already have attempted to undermine North Korea's nuclear and missile programme in this way, although details are scarce.[86] It is possible to envisage a scenario in which AI and CNOs are used to find vulnerabilities or create weaknesses that can be exploited in sensitive nuclear systems, and machine learning and autonomy are then used to launch a nuclear capability-retarding manipulation campaign.[87]

Europe and cyber–nuclear risk reduction

While measures to mitigate these challenges are still in their infancy, EU member states and institutions have an important role to play in cyber–nuclear risk reduction. This might involve continued work through the UN Group of Governmental Experts to establish general cyber norms, and more focused risk reduction dialogue between the nuclear-armed states.[88] Either the EU or the Organization for Security and Co-operation in Europe (OSCE) could use its good offices to promote dialogue and seek common interests, or they could even produce joint threat assessments in this space. Indirectly, this could involve working with NATO, Russia and the USA to build mechanisms for secure communications and clear signalling; increase transparency; build time, resiliency and redundancy into nuclear operations and relationships; and find ways to ameliorate some of the pressures driving nuclear modernization and complexity. European states might also seek to promote through the CD the idea of a moratorium on hacking into nuclear command and control systems, or to issue joint declarations about the risks of the cyber–nuclear interface.

VII. CONCLUSIONS AND RECOMMENDATIONS FOR EUROPEAN POLICYMAKERS AND PROFESSIONALS

The way that nuclear weapons are thought about and managed is being challenged by a perfect storm of technological developments. This has created an emerging grey area and increasing indistinguishability between nuclear and conventional systems, a likelihood of less time for decision making and a more complex information environment in which to operate, as well as new pathways to escalation, miscalculation and entanglement—all of which could increase the risk of nuclear use. Nonetheless, these dynamics are more nuanced—and in some cases more marginal—than is sometimes suggested. Thus, while the cumulative challenges posed by this new technological environment are considerable and diverse, they should not be insurmountable.

The task ahead may look daunting but there are things that can be done now in Europe to minimize and mitigate some of these risks. An important starting point will be increasing understanding and awareness, and addressing the worst-case scenario thinking that often fails to take account of the nature and nuance of some of the technological developments discussed above. For some technologies it is the methodology rather than the inherent nature of the nuclear risk that is changing, and these developments are likely to pose different questions for different actors. It is also important to remember that technological developments and risks do not occur in a political vacuum. In this way, ongoing dialogue and the establishment of norms and confidence-building measures across the nuclear space are as important as formal treaties or the implementation of restrictions on certain technologies—especially given that perceptions of technical trajectories will probably matter as much as, if not more than, technical realities. Moreover, future mechanisms of control, restraint and risk

[86] Sanger, D. E. and Broad, W. J., 'Trump inherits secret cyber war against North Korean missiles', *New York Times*, 4 Mar. 2017.

[87] Avin, S. and Amadae, S. M., 'Autonomy and machine learning at the interface of nuclear weapons, computers and people', eds Boulanin et al. (note 47), pp. 109–111.

[88] UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', [n.d.].

reduction might not look like those of the past. With all this in mind, this paper makes seven recommendations:

1. European leaders should encourage Russia and the USA to continue to pursue limits on deployed nuclear forces, and to include hypersonic weapons in current and future arms control agreements beyond the now extended New START. All states developing hypersonic weapons should be encouraged to keep nuclear and conventional delivery vehicles separate, distinguish clearly between tactical and strategic applications and, where possible, increase the time it takes to launch them. Serious thought might be given to an agreement not to deploy hypersonic weapons in Europe.
2. European NATO member states should work to ensure that future NATO and US plans in Europe are limited to specific threats and, if possible, coordinated with Russia. Transparency in *intentions* as well as *capabilities* is key to minimizing disruption.
3. The EU should take the lead in seeking to ban autonomous *nuclear*-armed delivery systems. At the same time, experts across Europe working on AI and automation should continue to reach out to brief policymakers on these issues in order to ensure the deepest understanding possible.
4. Building on the draft proposal for an International Code of Conduct for Outer Space Activities, the EU, the OSCE and other influential non-governmental actors in Europe should continue to pursue confidence building and elite-level education on the uses of outer space and the escalatory potential of counterspace operations. This might include working towards a moratorium on ASAT system testing and perhaps a ban on deploying direct-ascent ASAT weapons.
5. Influential officials and leaders across Europe should encourage Russia, the USA and possibly other nuclear-armed states to consider a moratorium on targeting nuclear command and control systems with CNOs.
6. Those directly involved in minimizing the nuclear risks posed by emerging and disruptive technology should avoid the pitfalls of viewing technological challenges in isolation or restricting risk analysis to 'domains'. Instead, these challenges are better viewed through a lens that focuses on pathways to escalation and nuclear use.
7. Governmental and Track 1.5 and 2 dialogues on strategic issues must continue across Europe and particularly with partners in Russia and the USA. The EU has a pivotal role to play in reducing the political pressures that underpin many of the challenges and risks noted in this paper, not least by facilitating the exchange of opinions, driving initiatives that help to build trust, and using its good offices to support the development of shared solutions.

There is still time to confront the range of nuclear challenges discussed in this paper and to formulate new mechanisms for management and control, but this will take genuine political will. Europe can and should become the engine for the development of a new edifice to manage global nuclear risks.

ABBREVIATIONS

ABM Treaty	1972 Treaty on the Limitation of Anti-Ballistic Missile Systems
AI	Artificial intelligence
ALTBMD	Active Layered Theatre Ballistic Missile Defence
BMD	Ballistic missile defence
C3	Command, control and communications
CD	Conference on Disarmament
CEP	Circular error probable
CNO	Computer network operation
DEW	Directed energy weapon
ELINT	Electronic intelligence
EU	European Union
GEO	Geostationary orbit
HCM	Hypersonic cruise missile
HGV	Hypersonic glide vehicle
INF Treaty	1987 Treaty on the Elimination of Intermediate-Range and Shorter-Range Missiles
ISR	Intelligence, surveillance and reconnaissance
LAWS	Lethal autonomous weapon systems
LEO	Low earth orbit
MARV	Manoeuvrable re-entry vehicle
MEO	Medium earth orbit
NATO	North Atlantic Treaty Organization
New START	2010 Treaty on Measures for the Further Reduction and Limitation of Strategic Offensive Arms
NPT	1968 Treaty on the Non-Proliferation of Nuclear Weapons
OSCE	Organization for Security and Co-operation in Europe
Outer Space Treaty	1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies
SDI	US Strategic Defense Initiative
UAV	Unmanned aerial vehicle

This document has been produced with the financial assistance of the EU. The contents are the sole responsibility of the EU Non-Proliferation and Disarmament Consortium and can under no circumstances be regarded as reflecting the position of the EU.

A EUROPEAN NETWORK

In July 2010 the Council of the European Union decided to support the creation of a network bringing together foreign policy institutions and research centers from across the EU to encourage political and security-related dialogue and the long-term discussion of measures to combat the proliferation of weapons of mass destruction (WMD) and their delivery systems. The Council of the European Union entrusted the technical implementation of this Decision to the EU Non-Proliferation Consortium. In 2018, in line with the recommendations formulated by the European Parliament the names and the mandate of the network and the Consortium have been adjusted to include the word 'disarmament'.

STRUCTURE

The EU Non-Proliferation and Disarmament Consortium is managed jointly by six institutes: La Fondation pour la recherche stratégique (FRS), the Peace Research Institute Frankfurt (HSFK/ PRIF), the International Affairs Institute in Rome (IAI), the International Institute for Strategic Studies (IISS), the Stockholm International Peace Research Institute (SIPRI) and the Vienna Center for Disarmament and Non-Proliferation (VCDNP). The Consortium, originally comprised of four institutes, began its work in January 2011 and forms the core of a wider network of European non-proliferation and disarmament think tanks and research centers which are closely associated with the activities of the Consortium.

MISSION

The main aim of the network of independent non-proliferation and disarmament think tanks is to encourage discussion of measures to combat the proliferation of weapons of mass destruction and their delivery systems within civil society, particularly among experts, researchers and academics in the EU and third countries. The scope of activities shall also cover issues related to conventional weapons, including small arms and light weapons (SALW).

www.nonproliferation.eu

EU Non-Proliferation and Disarmament Consortium

Promoting the European network of independent non-proliferation and disarmament think tanks

FONDATION pour la RECHERCHE STRATÉGIQUE

FOUNDATION FOR STRATEGIC RESEARCH

www.frstrategie.org

PRIF HSFK
Peace Research Institute Frankfurt
Hessische Stiftung Friedens- und Konfliktforschung

PEACE RESEARCH INSTITUTE FRANKFURT

www.hsfk.de

iai Istituto Affari Internazionali

INTERNATIONAL AFFAIRS INSTITUTE

www.iai.it/en

IISS

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES

www.iiss.org

sipri

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

www.sipri.org

VCDNP
Vienna Center for Disarmament and Non-Proliferation

VIENNA CENTER FOR DISARMAMENT AND NON-PROLIFERATION

www.vcdnp.org

© EU Non-Proliferation and Disarmament Consortium 2021