NEW TECHNOLOGIES AND NUCLEAR STRATEGY

INITIATIVES FOR NUCLEAR DISARMAMENT

IDN
Initiatives pour le désarmement nucléaire.

Initiatives pour le désarmement nucléaire

Initiatives for Nuclear Disarmament

14 rue Brochant

BAL N°17

75017 Paris

Email: idn@idn-france.org

Website: https://www.idn-france.org/

Twitter: @IDN_Nucleaire

Initiatives pour le désarmement nucléaire (IDN, Initiatives for Nuclear Disarmament) is a non-profit organization.

← *Cover photo:*

Félix Anthonysamy

To cite this article:

NORLAIN Bernard (dir.), "*Les nouvelles technologies et la stratégie nucléaire*", Initiatives pour le désarmement nucléaire, Paris, November 2021.

NEW TECHNOLOGIES AND NUCLEAR STRATEGY

TABLE OF CONTENTS

FOREWORD

This study is published shortly after Paul Quilès, President and founder of IDN, and Michel Drain, a member of the association's board, passed away.

It is dedicated to them as a tribute to their tireless work and their invaluable contribution to our common struggle for a safer, more just and more peaceful world.

Despite their own courageous battle with the disease, Paul and Michel are behind this study.

They brought their knowledge, their convictions and their concerns for the security of humanity and the environment, threatened by nuclear weapons made even more dangerous and useless by new technologies.

Michel Drain had already expressed his fears on this subject in his book co-edited with Paul Quilès in 2018, "L'Illusion nucléaire" (Ed. L'Harmattan).

Paul Quilès wrote the chapter on war in space for this study, which will be his last publication.

Drawing on his experience as a former defence minister, he paints a disturbing picture of the arms race in space.

Indeed, nuclear strategy is dependent on space systems, which increases the temptation for nuclear powers to destroy the systems of adversaries, further increasing the risk of nuclear catastrophe.

Let us hope that the wisdom contained in these analyses and recommendations will be convincing to our leaders and decision-makers.

The IDN team

1. INTRODUCTION

Source: iStock

In recent years the development of new advanced technologies has given rise to numerous questions about the profound changes they imply for all aspects of our way of life. An abundant literature has thus appeared, devoted to the perspectives opened up by these emerging technologies that have the potential to both improve our lives and threaten our security.

Among all these comments, the idea of the disruptive impact of these new technologies on geopolitics and therefore on security policies quickly gained consensus: "*the race for technological domination is inextricably linked to the evolution of geopolitics*"[1].

In an interconnected world where the ability to control information is becoming an existential issue in a complex world order under pressure from heightened international competition, the advantages that technological supremacy can provide make it a key strategic issue.

For this reason, Initiatives pour le Désarmement Nucléaire (IDN) has decided to examine the impact of new technologies on the nuclear strategy of states armed with nuclear weapons (nuclear-weapon states) and their allies. While this strategy is commonly referred to as "*nuclear deterrence*", in reality is nothing more than a **strategy of nuclear terror**.

The study also highlights the ethical, societal and security issues raised by the new technologies. The application of artificial intelligence (AI) combined with other technologies, biotechnological innovations and quantum physics, to name but a few of these developments, highlights the need for – but also the difficulty of – global control and regulation.

[1] SMOLAR Piotr, "Preface," in SMOLAR Piotr (ed.), *Le Monde en 2040 vu par la CIA*, Equateurs Document, June 2021.

This paper focuses on eight technologies that we consider to be essential because of their innovative and forward-looking characteristics: hypersonic missiles, directed-energy weapons, cyber threats, space warfare, artificial intelligence, biotechnology, nanotechnology, and quantum technology. It does not claim to be exhaustive or to be a scientific study, but focuses on an aspect that is very rarely examined, that of the impact of new technologies on nuclear strategy.

2. HYPERSONIC MISSILES

Marc Finaud

Abstract: The United States pretends to be concerned about the future Russian and Chinese deployment of hypersonic missiles capable of neutralizing any missile defence system, even though it too is investing in this technology. Confidence in "nuclear deterrence" to prevent a first strike has already been weakened by the use of missile defence systems. The escalation resulting from the current race to circumvent these systems is a dangerous gamble that can only encourage offensive action and could lead to global cataclysm.

Boeing X51-A WaveRider scramjet tested by the US Air Force.
Source: US Air Force

2.1 Definitions and characteristics

A hypersonic missile (or "vehicle") can be defined in relation to a ballistic missile by several characteristics:

- Like an aircraft, it takes off from a land, sea or airborne **platform**.
- It flies in near space (below 100 km in altitude) at **speeds** above Mach 5 (five times the speed of sound, or 6,150 km/h) and as high as Mach 20 (24,696 km/h) or more.
- Its form of propulsion is not a turbojet or a classic jet engine (because of the lack of oxygen at its operational altitudes), but a *superstator jet* or ramjet with a supersonic combustion system ("**scramjet**").
- Like a ballistic missile, it is capable of carrying either a conventional explosive or **nuclear warhead**.

The **hypervelocity** that characterizes a hypersonic missile is not sufficient to distinguish it from a ballistic missile, part of whose trajectory (final phase) may also be at supersonic speed. A hypersonic missile can also fly at a speed greater than the speed of sound in only part of its trajectory (in the take-off or propulsion phase, intermediate phase, or final phase). The main difference lies in its **manoeuvrability**, which is comparable to that of a cruise missile, whose trajectory, unlike that of a ballistic missile, is not predictable.

However, the combination of **hypervelocity** and **manoeuvrability** makes it more difficult for the missile to hit the target, which leads to a reduction in the speed of the vehicle in the final phase, hence the use of glide vehicle technology for more efficient guidance.

The **range** of a hypersonic missile depends on several factors: the type of launch platform, the launch speed, the number of manoeuvres carried out in flight, the flight altitude, the duration of the passage through the atmosphere, the weight of the warhead, etc.

Compared to a ballistic missile, in addition to the combustion superstator, a hypersonic missile requires **advanced technology**, including:

- Specific aerodynamics;
- Heat-resistant materials for aerothermal protection;
- Advanced navigation and stabilization systems, etc.

There has been no shortage of technological challenges since the first hypersonic missile research programmes were launched in the 1990s:

– The superstator jet's combustion system cannot work efficiently below Mach 1, which means that it has to be combined with another propulsion system (turbojet or aircraft launch) for its sonic or subsonic flight phases.

– Guidance systems such as inertial navigation (INS) lose accuracy over long distances and GPS is vulnerable to hacking.

– The missile's aerodynamics require a thin envelope that is sensitive to high temperatures.

– Stabilization in the various phases of the flight remains difficult to control.

CATEGORY	FINAL SPEED	PROPULSION	EXAMPLE
Supersonic	Mach 1 to Mach 3	Propeller, turbojet, ramjet	BrahMos anti-ship cruise missile (Russia-India); X-51 WaveRider unmanned aircraft (USA)
Hypersonic cruise missile	Mach 5	Ramjet, superstator reactor	Kinjal Kh-47M2 high-accuracy air-to-surface ballistic missile (Russia); Zircon 3M22 hypersonic cruise missile (Russia)
Hypersonic glider	Mach 20	Thruster and glider	Manoeuvrable re-entry ballistic missile (MARV): Avangard Hypersonic Glider (Russia); DF-17 Hypersonic Glider (China); Falcon HTV-2 Hypersonic Glider (USA)
Intercontinental ballistic missile/submarine-launched missile	Mach 27	Thruster, independently loaded re-entry vehicle (ILRV)	Minuteman III and Trident I D-5 ballistic missiles (USA); SS-19 (Russia), etc.

Nuclear missile categorization table. © IDN 2021.

2.2 Impact on "*nuclear deterrence*"

The concept of "*nuclear deterrence*" as it was forged during the Cold War was based on the balance of terror and the concept of "mutual assured destruction" (MAD). According to this doctrine, the capacity to respond to an attack (a first strike) would be so devastating that no rational aggressor could risk being annihilated, and would therefore be deterred from carrying out a first strike. But the entire history of both the Cold War and the present period is also the history of a frantic race between offensive and defensive weapons.

In the 1960s both the United States and the Soviet Union developed and deployed defensive missiles capable of intercepting their opponent's offensive intercontinental ballistic missiles (IBMs). As a result, in order to counteract these defences, offensive missiles were equipped with multiple nuclear warheads (MIRVs) and countermeasures from the 1970s onwards, rendering any defensive system unaffordable or ineffective. This stalemate continued until the day when the two superpowers decided to negotiate in parallel the limitation of their strategic offensive arsenals (SALT Treaty of 1972) and their anti-missile systems (ABM Treaty of 1972). Introducing a missile defence against a nuclear strike was tantamount to recognizing the intrinsic weakness of deterrence, since in this scenario it would not have prevented a first strike. At most, defensive systems were designed to limit the destruction of a first strike and preserve retaliatory capabilities.

But the race was not stopped: US president Ronald Reagan, sceptical of the concept of deterrence, launched his famous "*Star Wars*" project or Strategic Defence Initiative (SDI) in the early 1980s, which aimed to make nuclear weapons obsolete by providing total protection of US territory against a Soviet attack. Overly ambitious and technically and financially unfeasible, this project was abandoned in favour of more limited missile defence programmes, in particular, from the US point of view, to protect itself not against IBMs, but against missiles fired by "rogue states" such as Iran or North Korea, an argument used by President George W. Bush to withdraw the United States from the ABM Treaty in 2002. The Russian response was swift: Moscow then denounced the START II Treaty, which had included a ban on MIRVs, thus relaunching the offensive-versus-defensive arms race.

Despite regular denials by Washington and NATO, the deployment of a missile defence system in Europe (EPAA), launched by President Obama in 2009, could not prevent Russia from perceiving it as a threat to what an understated euphemism describes as its "*strategic stability*", i.e., its ability to retaliate against an attack by the United States or NATO. It is therefore not surprising that the Russian president, Vladimir Putin, responded by announcing

with great fanfare on 1 March 2018 the launch of new offensive programmes, among them the "unlimited" range Sarmat intercontinental cruise missile, equipped not only with MIRVs and countermeasures, but also capable of launching "Vanguard" *hypersonic* vehicles ("boost-glide vehicles") capable of evading any missile defence system. As Putin clearly stated, this massive investment was a response to the US withdrawal from the ABM Treaty, but also to the Pentagon's plan to deploy a conventional long-range precision missile ("*Prompt Global Strike*"), perceived by Moscow as a threat to its nuclear missile sites.

In response, the United States described the announcements as "*irresponsible*" and stressed that the ambition of US missile defence systems was limited to providing protection against Iran and North Korea. The United States is nevertheless pursuing a programme to develop hypersonic (Mach 5) missiles designed to respond not only to Russian weapons, but also to those of China, which are considered to be very advanced. Like India, France is not to be outdone, since it is developing the ASN4G (fourth-generation air-to-ground nuclear missile), which is intended to succeed the ASMP-A missile. The main criticism of these technological choices is that the missiles in question are likely to be used as delivery vehicles for both conventional and nuclear weapons, and therefore run the risk of provoking a nuclear response to a conventional strike by mistake.

Indeed, the risk of nuclear war is even greater because of the **dual nature of hypersonic missiles**: a conventional attack, for example against command-and-control centres, land- or space-based early warning systems, surface missile silos or submarines, communications networks, or aircraft carriers, could result in an escalation to nuclear war.

It is precisely in order to circumvent "*conventional*" missile defences that Russia and China have invested in hypersonic missiles, which are supposed to prevent any attempts to neutralize them, and thus reinforce the possibility of a first strike – except that, in order to destroy all of the adversary's response capability, it would be necessary to be able to destroy not only all of its land-based sites (including command-and-control sites), but also its submarine-based capabilities, which is currently still impossible. In short, **neither offensive nor defensive weapons are capable of preventing a nuclear war**.

Although Russian and Chinese investments in hypersonic missiles are huge, at this stage they seem more intended to send a message to the United States along the lines of: "*give up your missile defence to allow our deterrence ("second strike") to work or we will threaten your own deterrence with our first strike capabilities*". This is a dangerous game of poker that can only lead to escalation.

Beyond any consideration of the absurdity and ineffectiveness of "*nuclear deterrence*", it is therefore high time – since the development and deployment of these systems will take a long time – to break this vicious circle and launch a disarmament race. The best assurance that nuclear weapons will never be used is undoubtedly their elimination. But we know that elimination is still some time away.

In the meantime, in order to prevent the outbreak of the nuclear cataclysm – even if it is accidental or involuntary – it is crucial to return to the mechanisms that have previously allowed for balance and stability:

- Limiting anti-missile systems;
- Banning multiple nuclear warheads (MIRVs);
- Enhancing transparency in ballistic missile and space activities; and
- Negotiating a ban on the deployment of nuclear warheads on hypersonic delivery systems, in order to confine this technology to the realm of conventional defence and prevent a dangerous drift towards nuclear confrontation.

2.3 Bibliography

- BAROTTE, Nicolas, "Les grandes puissances dans la course aux missiles hypersoniques," *Le Figaro* (August 20, 2020), https://www.lefigaro.fr/international/les-grandes-puissances-dans-la-course-aux-missiles-hypersoniques-20200820
- BORRIE, John, PORRAS, Daniel, *The Implications of Hypersonic Missiles for International Stability and Arms Control,* UNIDIR (October 2019), https://unidir.org/sites/default/files/2019-10/Hypersonic%20Weapons%20Tabletop%20Exercise%20Report.pdf
- FINAUD, Marc, "Hypersonic Missiles and Nuclear Deterrence: A Dangerous Poker Game," IDN (August 1, 2018), https://www.idn-france.org/etats-unis/missiles-hypersoniques-et-dissuasion-nucleaire-un-jeu-de-poker-dangereux/
- GUDRUB, Mark, "Going Too Fast: Time to Ban Hypersonic Missile Test?", *The Bulletin of the Atomic Scientists* (September 2015), https://thebulletin.org/2015/09/going-too-fast-time-to-ban-hypersonic-missile-tests-a-us-response/

- McWHINNEY, Mark, *The Risks of Hypersonic Weapons,* Canada, Ploughshares Spotlight (April 2020), https://ploughshares.ca/wp-content/uploads/2020/12/Spotlight_Hypersonic-Weapons.pdf

- STEFANOVITCH, Dmitry, *Hypersonic Weapons and Arms Control*, Russian International Affairs Council (December 2020), https://russiancouncil.ru/en/analytics-and-comments/analytics /hypersonic-weapons-and-arms-control/

- TRACY, Cameron L., WRIGHT, David, "Modelling the Performance of Hypersonic Boost Glide-Missiles," *Science & Global Security*, vol. 28, no. 3 (April 2020), pp. 137-170, http://scienceandglobalsecurity.org/archive/2020/12/modelling_the_performance.html

3. DIRECTED-ENERGY WEAPONS

Jacques Fath

Abstract: Directed-energy weapons (laser or electromagnetic pulse weapons) are part of electronic warfare technologies. They offer multiple capabilities, in particular anti-missile capability or the ability to paralyze communication or control-and-command systems. These weapons have a strong strategic potential, for example by neutralizing the functioning of or destroying the most sophisticated weapons and defence systems, including aircraft and satellites. They make possible what can be called localized strategic chaos (adversely affecting military zones or bases) by interrupting the functioning of computers and computer systems or the distribution of electricity, and making it difficult or impossible for a country to control its own forces. Contrary to some theories, directed-energy weapons do not constitute an "alternative to deterrence", but they are likely to modify its terms, and to affect its logic and relevance by giving those who possess them a superior capacity to neutralize opponents and provide the conditions for an effective nuclear first strike.

The US Navy's AN/SEQ3 laser system.
Source: J. F. Williams / US Navy

3.1 Useful definitions

A directed-energy or radiation weapon is a weapon that can project a beam of laser or microwave waves at the speed of light towards a target, possibly (in the case of lasers) with a high degree of precision. Such weapons have several advantages: lightning speed, adjustable power, precision and economy in their use (they need no ammunition). They can reach very distant targets, and can blind or neutralize land, airborne or naval weapons systems and information and communication systems.

3.1.1 Radiation weapons

Radiation weapons are being developed by countries with the necessary research and development capabilities, in particular the major powers (the United States, China, Russia, France, etc.), which are engaged in a rapid and intense arms race in this field as in many others. However, the relatively low cost of such weapons compared with today's sophisticated conventional weapons could be of interest to a number of countries wishing to have such advanced systems with deterrent ability.

These weapons are now entering the experimentation or integration phases in armies and open up the possibility of electronic warfare.

3.1.2 Laser weapons

Laser weapons[2] work by concentrating a beam of light on a surface, for example the surface of a missile. The thermal effect can perforate the surface at which it is aimed, damage the missile and prevent it from operating. The higher the level of energy released, the larger the targets that can be attacked. However, the effectiveness of these weapons depends on variations in the environment: fog, humidity, sandstorms, etc. These conditions present a number of technical difficulties, in particular the need for considerable energy to be produced if the weapon is to be effective. As a result, the system can be too cumbersome and heavy for some airborne and other vehicles. The military applications of lasers are numerous: telemetry, fire control assistance, target lighting, electronic sensor glare, secure telecommunications, experimental nuclear simulation (megajoule laser), etc.

[2] LASER stands for "*light amplification by stimulated emission of radiation*".

3.1.3 Microwave weapons

Microwave weapons operate by emitting beams or pulses of high-frequency waves (or microwaves). The electromagnetic pulse has the potential to degrade or even paralyze electronic circuits, computer systems and computers, satellites, communication and command-and-control systems, and critical (life-saving) civilian or military infrastructure, theoretically without collateral damage, but potentially affecting civilians.

3.2 Laser weapons and their relationship to nuclear power

Laser technology has multiple military applications, including its use in space (satellite-to-satellite communications) and for terrestrial links with satellites, for example to transmit earth observation data, which indicates the strategic potential of this technology. The laser is also (for at least the last ten years) being tested for communications between submarines, and between surface vehicles and submarines. Research is under way in particular to overcome the limits inherent in the turbulence of the marine environment. The use of lasers for this type of communication is likely to provide reliable, high-throughput and secure communication, which may represent a strategic advantage. In these two configurations (space and marine environment), the advantages of this technology seem obvious, for example its ability to contribute to the control of nuclear forces (strategic air forces and ballistic missile submarines like the French SNLE class of submarines).

Anti-missile lasers could be used to protect support aircraft (tankers and intelligence aircraft) during air operations in conflict situations. The use of such lasers could thus be linked to exercises or strategic operations with a nuclear dimension.

With the ability to aim a high-powered laser beam at a cruise or ballistic missile, the laser could acquire an air-threat-elimination or missile-defence capability suitable for use against all kinds of conventional, hypersonic and even nuclear weapons. But this is still at the experimental or speculative stage.

3.3 Electromagnetic pulse weapons and their relationship to nuclear weapons

The potential effectiveness of these weapons against infrastructure (strategic military bases, for example) or certain weapons is becoming clearer, since existing systems are increasingly dependent on their electronic devices and means of transmission. Electromagnetic pulse weapons therefore have the strategic capacity to hinder or even neutralize the functioning of the most sophisticated weapons and defence systems, including aircraft and satellites involved in nuclear missions. Aircraft with a nuclear mission capability – e.g. the Rafale and the planned SCAF[3] – could be neutralized because of their vulnerability to electromagnetic weapons.

It is possible to use microwave or microwave weapons to create localized strategic chaos by interrupting communications, computer systems and power distribution systems; paralyzing command systems; and seriously limiting a country's ability to control its own forces, hence the temptation to design sufficiently powerful offensive devices capable of multiplying the effects of the electromagnetic pulse. Contrary to some theories, directed-energy weapons do not constitute an "*alternative to nuclear deterrence*", but they are likely to modify its terms and to affect its logic in a particular way by conferring on those who possess them a superior capacity to neutralize enemy defences, and thus offer the possibility of a first-strike initiative.

3.4 What changes do directed-energy weapons bring about?

High technology, as a force multiplier and a revolution in capabilities, allows the development of new categories of weapons capable (apart from nuclear weapons) of carrying out strikes and producing damage qualitatively superior to what was previously possible. We are therefore entering another dimension. However, these are not weapons of deterrence in the usual strategic sense, but new means of warfare, in this case electronic warfare.

It must be remembered that, by definition, nuclear weapons and conventional weapons belong to two different military and strategic orders, but there are structural continuums in

[3] Système de combat aérien du futur (Future Air Combat System): this is a very complex European aircraft project that is supposed to become operational in 2040 and is to be built by defence industrial groups from France, Germany and Spain.

defence systems and strategies. Today, radiation weapons, like other high-tech weapons, could significantly change this basic situation. High technology – and in particular radiation weapons – will introduce both new vulnerabilities and new specific means of protection and effectiveness for infrastructure, delivery systems and command systems, especially nuclear weapons. High technology is therefore being increasingly integrated into defence systems.

At a time when there is renewed interest in tactical nuclear weapons, which are more likely to be used effectively, greater integration between conventional, nuclear and high-tech defence systems could mean a loss of the (further) relevance of deterrence in the strict or traditional sense, in favour of a new conception of warfare whereby all means are being integrated into all fields. There is a danger that the nuclear risk will be amplified in this way.

The impact of directed-energy weapons on nuclear military power is therefore real, as is that of hypersonic missiles, artificial intelligence (AI) and cyber defence. This is not a form of "*overtaking*" of nuclear military power by high technologies, but it does lead to major transformations in many forms of warfare.

The new weapons systems are based on very high-level technologies involving greater speed, power, precision, adaptability and autonomy. In the new strategic context, major wars and so-called high-intensity conflicts are becoming all the more conceivable (or even probable?) as digital technology, AI, growing confrontation in cyberspace and outer space, and robotization risk feeding through the ongoing process of dematerialization the dangerous illusion of being able to "*distance*" countries from war and future shocks, and the illusion of a decrease in the risks war poses to human life, in particular the lives of soldiers. There is therefore the very real risk of the wars of today and tomorrow rapidly escalating because of this perceived lack of risk, possibly with nuclear dimensions.

An attempt can be made to differentiate the impact of high technologies according to their actual or potential characteristics and functions. Like AI, cyber and quantum computing will certainly have a transversal or even global impact on highly integrated defence systems. As for hypersonics, it could be a "*game changer*" in the sense of providing a powerful potential for strategic disruption.

It is quite complicated, and perhaps not particularly necessary (although it does help with the analysis) to establish hierarchies or functional calibrations between technologies. In reality, it is the innovative configuration of so-called multi-domain operations (or collaborative warfare) that is thus made possible by the technologies that enable and accelerate this highly integrated form of warfare, i.e., a "*global*" war made possible in particular by the technologies

that provide the sophisticated instruments for a very wide-ranging conflict. In this global war, it is above all the integration and complementarity of all defence components that will determine the new standards of military power. Technological and military "*performance*" will be global. Superiority will depend on the ability to master this integration and synchronization of warfare operations.

Clearly, we are only in the early stages of this future type of warfare, of which technology is only one aspect. A war of the future will be the product of both technological change and the radical transformation of the global geopolitical context.

We are entering a phase of exacerbated competition and confrontation dominated by the major powers (the United States, China, Russia, etc.) combined with the perilous collapse of the existing international security architecture (particularly "*arms control*") and multilateralism. The war of the future that is taking shape means that we are moving into a new period of international interaction, new risks, and transformed international security issues in the context of the end of the international order established under US hegemony after 1945.

3.5 The French response

France has been very committed to high-tech military equipment for several years. In 2018 it set up the Defence Innovation Agency, and in 2019 it created the Red Team, which, with the help of experts, authors and science fiction writers, was responsible for coming up with "*disruptive*" ideas and a forward-looking military vision. In 2020 France set up the Defence Ethics Committee, which was concerned in particular with the consequences of the emergence of new defence technologies. With regard to directed-energy weapons, it is testing, in particular for the French navy, a "Helma-P" laser turret designed to track and shoot down targets in flight such as drones.

Yet the White Papers on Defence and National Security of 2008 and 2013 and the Strategic Review of 2017 hardly comment on French projects and government interest in high-tech military developments in general. In his official speeches on defence, President Emmanuel Macron has not said a word about these issues. The armed forces minister, Florence Parly, never refers at any length to the substance of the problem.

As for the European Union, it has developed a project for an "*electronic warfare capability",* adopted on 19 November 2018 in the framework of the system of Permanent

Structured Cooperation, with a view to creating a "*joint electronic warfare unit*". The participating countries in this project are Germany and the Czech Republic as lead nations.[4]

The significance of the emergence of high-tech military equipment in the international order and their integration into France's defence policy, which is much more voluntarist than in the past, cannot be dealt with in terms of the quasi- or semi-confidentiality that currently dominates the official discourse – or, rather, the official non-discourse. It is as if French political leaders want to hide the nature and scope of their choices ... and their difficulties.

3.6 Bibliography

Books and general documents

- ASSOCIATION DES AUDITEURS ET CADRES DES HAUTES ETUDES DE L'ARMEMENT (AACHEAR), *Géostratégie et armements au XXIe siècle*, La Documentation française, Collection armements et sécurité, 2014, 570 p.

- BOUTHERIN, Grégory, "Un nouveau phénomène conceptuel made in USA : le combat multidomaine", *Areion24News*, January 9, 2017, https://www.areion24.news/2017/01/09/nouveau-phenomene-conceptuel-made-in-usa-combat-multidomaine/

- U.S DEPARTMENT OF DEFENSE, "*Directed Energy Futures 2060. Visions for the next 40 years of U.S. Department of Defense Directed Energy technologies*", https://www.afrl.af.mil/Portals/90/Documents/RD/Directed_Energy_Futures_2060_Final29June21_with_clearance_number.pdf

- FATH, Jacques, "Les très hautes technologies dans une nouvelle course aux armements", in FATH Jacques, *Chaos. La crise de l'ordre international libéral. La France et l'Europe dans l'ordre américain*, Éditions du Croquant, 2020, pp. 101-136.

[4] See *European Defence: The Challenge of Strategic Autonomy*, Information Report no. 626 (2018-2019) by Ronan Le Gleut and Hélène Conway-Mouret on behalf of the Senate Committee on Foreign Affairs, Defence and Armed Forces, 3 July 2019. Annex 2, PSC projects, https://bit.ly/3gmxWVN.

– FAURY, Etienne, "Les opérations multidomaines: une révolution militaire," *Revue Défense nationale*, 2020, https://www.defnat.com/e-RDN/vue-article-cahier.php?carticle=235

– FONTAINE, Bernard (pref. PARRAUD, Paul), *Les armes à énergie dirigée: mythe ou réalité?,* L'Harmattan, October 2011.

– LAURENT, Boris, "From Battle to Multi-domain Operations: Preparing for the War of the Future," Areion24.news, July 22, 2020, https://www.areion24.news/2020/07/22/de-la-bataille-aux-operations-multidomaines-se-preparer-pour-la-guerre-du-futur/

– LELE, Ajay, *Quantum Technologies and Military Strategy*, Springer, 2021.

– MISSIROLI, Antonio, "Game of Drones? Or How New Technologies Affect Deterrence, Defence and Security," *NATO Review*, May 5, 2020, https://www.nato.int/docu/review/fr/articles/2020/05/05/game-of-drones-ou-comment-les-nouvelles-technologies-influent-sur-la-dissuasion-la-defense-et-la-securite/index.html

– SECRETARIAT GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE (SGDSN), "*Chocs futurs – Étude prospective à l'horizon 2030: impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité,*" 2017, http://www.sgdsn.gouv.fr/rapport_thematique/chocs-futurs/

Defence industry sources

– CAILABS, "AED Directed Energy Laser Weapons", https://www.cailabs.com/application/armes-laser-a-energie-dirigee/

– CAILABS, "Underwater Laser Communications: Tilba Makes Underwater Laser Communications More Reliable by Compensating for Turbulence," https://www.cailabs.com/application/communications-laser-sous-marines/

– LOCKHEED MARTIN, "New Age Threats Require New Age Defenses: Directed Energy Technology Has Advanced from the Lab and Is Now Ready for the Field," https://www.lockheedmartin.com/en-us/capabilities/directed-energy.html

– LOCKHEED MARTIN, "Tactical Airborne Laser Pods Are Coming," https://www.lockheedmartin.com/en-us/news/features/2020/tactical-airborne-laser-pods-are-coming.html

– THALES DEFENSE AND SECURITY, "Optronic Systems for Air Forces," https://www.thalesgroup.com/fr/activites/defense/air-forces/systemes-optroniques-forces-aeriennes

Specific articles and topics

– ARMEE DE L'AIR ET DE L'ESPACE, "Chammal: First Operational Mission of the Talios Pod" (December 7, 2020), https://www.defense.gouv.fr/air/actus-air/chammal-premiere-mission-operationnelle-du-pod-talios

– BOURDON, Pierre, *Technologies laser pour applications militaires*, thesis (optics/photonics), Université Paris-Sud, Faculté des Sciences d'Orsay, 2016, https://hal.archives-ouvertes.fr/tel-01371573/document

– COHEN, Rachel S., "Some Directed-Energy Weapons Show Promise While Others Slow," *Air Force Magazine* (July 7, 2020), https://www.airforcemag.com/some-directed-energy-weapons-show-promise-while-others-slow/

– FENG, John, "China Developing Unique Laser Gun for Faster Hypersonic Missiles and Planes," *Newsweek* (July 27, 2021), https://www.newsweek.com/china-developing-unique-laser-gun-faster-hypersonic-missiles-planes-1613374

– KELLER, John, "Air Force Asks Industry for Laser Weapons and High-Power Micro-Wave to Defend against Cruise Missiles," *Military & Aerospace Electronics* (September 10, 2019), https://www.militaryaerospace.com/power/article/14039601/laser-weapons-cruise-missiles-highpower-microwaves

– KELLER, John, "Wanted: High Power RF and Microwave Amplifiers for Electronics-Killing Electronic Warfare (EW) Systems," *Military & Aerospace Electronics* (March 11, 2021), https://www.militaryaerospace.com/rf-analog/article/14199141/rf-and-microwave-amplifiers-electronic-warfare-ew

– "Laser Weapons: Towards a Timid Entry into the Naval Combat Arena on the Eve of the Next Decade," *Defense and Industry*, no. 12 (October 2018),

https://www.frstrategie.org/sites/default/files/documents/publications/defense-et-industries/2018/12-5.pdf

- PARDE, Nathan, "Lincoln Laboratory Advances Undersea Optical Communications: Researchers Are Applying Narrow-Beam Laser Technology to Greatly Improve Communications between Underwater Vehicles," *MIT Lincoln Laboratory News* (August 1, 2018).

- VERGUN, David, "DoD Officials Discuss Framework for Advancing Directed Energy Weapons," *DoD News* (August 11, 2020), https://www.defense.gov/Explore/News/Article/Article/2309408/dod-officials-discuss-framework-for-advancing-directed-energy-weapons/

- VERGUN, David, "Ready, Aim, Fire: Hypersonics, Directed Energy, Lasers," *DoD News* (April 25, 2019), https://www.defense.gov/Explore/News/Article/Article/1824471/ready-aim-fire-hypersonics-directed-energy-lasers/

- WILSON, J. R., "The New Era of High-Power Electromagnetic Weapons," *Military & Aerospace Electronics* (November 19, 2019), https://www.crows.org/news/478754/The-new-era-of-high-power-electromagnetic-weapons.htm

- WOLF, Fabrice, "La vulnérabilité des avions ravitailleurs inquiète l'US Air Force," *Meta Défense* (September 24, 2020), https://www.meta-defense.fr/2020/09/24/la-vulnerabilite-des-avions-ravitailleurs-inquiete-lus-air-force/

- WOLF, Fabrice, "Les armées françaises se préparent à tester leurs premières armes laser de la PME orléanaise CILAS," *Meta Défense* (March 3, 2020), https://www.meta-defense.fr/2020/03/03/les-armees-francaises-se-preparent-a-tester-leurs-premieres-armes-laser-de-la-pme-orleanaise-cilas/

4. THE CYBER THREAT

Solène Vizier

Abstract: The advent of the digital age increases the risks caused by the pre-existing vulnerabilities of nuclear weapons systems and creates new threats. Communication and control systems can be hacked, while communication systems, missile telemetry, assembly facilities and autonomous robotic systems in the strategic infrastructure are vulnerable. The development of smart weapons, such as ballistic missile defences or satellite weapons, will have an impact on nuclear thinking and strategies. These new technologies may offer opportunities for "deterrence by denial": designed to intercept missiles or warheads after launch, they are also used to prevent nuclear weapons systems from functioning as intended. In short, the entire current nuclear strategy is being challenged.

Cyberwarfare officers.
Source: ASPI Strategist

Introduced into the national security lexicon in the early 1990s, the term "cyber" – the prefix of cybernetics – has become a generic expression used to signify the digital dimension of the concept it accompanies (cyber defence, cyber diplomacy, cyber terrorism, etc.). **The notion of "*cyber*" can be defined both as the emergence of a new digital context and as a new set of tools, dynamics and weapons.**

The advent of the digital age is now increasing the risks caused by pre-existing military vulnerabilities and creating new threats. The reliability and integrity of all aspects of nuclear weapons systems are now being questioned. **The hacking of these systems, which in the past seemed impossible, has now become a real risk.** The threat is compounded by the fact that nuclear weapons were created at a time when computing was in its infancy, and cyber risk has not been factored into the architecture of current nuclear weapons systems and strategies. And if nuclear weapons are meant to have a political rather than a military purpose – i.e., they are meant to keep the peace without ever being used – the barriers to their use are slowly being eroded.

The cyber challenge involves the command and control of all information technologies involved in nuclear weapons management. It operates in the four domains of the information environment:

- *Physical / mechanical:* physical infrastructure and equipment;
- *Logic:* the commands telling the hardware what to do and the software enabling the transmission, interpretation and sharing of information;
- *Informational:* the information and data that the system collects, stores, generates and uses to operate; and
- *Human/cognitive:* human beings and their interactions with hardware, software and information.

4.1 Cyber threats

Cyber threats encompass a broad spectrum of activities, ranging from simple hacking to denial-of-service attacks and from espionage to sabotage. Cyber risks have introduced new vulnerabilities into nuclear weapons systems, which are understood as weaknesses in an element of an industrial or information system. In its report *Cybersecurity of Nuclear Weapons*

Systems Threats, Vulnerabilities and Consequences, Chatham House's Department of International Security identified **13 areas that are vulnerable to cyber risks**, including various communication systems, missile telemetry data, cyber technologies in laboratories and assembly facilities, meteorological and targeting information from space systems or ground stations, and autonomous robotic systems in the strategic infrastructure. These vulnerable areas all have attack vectors through which a malicious actor can access sensitive information or create false information.

4.1.1 Cyber espionage

Often considered the second-oldest profession in the world, espionage is not a new challenge for nuclear weapons systems and contributed to nuclear proliferation in the 20th century. The second nuclear age (since 1991) presents two sets of challenges. For Andrew Futter, the first key development affecting nuclear espionage is the increasing use of digital computers for data storage. Scientific and technical material on nuclear testing, research and development data, weapons designs, military structures, and doctrines for weapons use are stored on digital networks. This makes it easier to access information, even though these computers are separate from the Internet and unsecured networks. A significant portion of nuclear espionage operations have involved insiders with access to poorly secured systems due to significant failures in cyber security and cyber hygiene. The second key development is the ability to access and target nuclear secrets remotely – as in the **SolarWinds** attack that notably affected the US National Nuclear Security Administration in early 2020.

4.1.2 Information handling and e-disability

The cyber threat affects nuclear risks in two main ways: **it compromises both nuclear weapons information and warning systems and nuclear weapons command-and-control systems**. Expert Andrew Futter points out that the first major challenge to nuclear weapons systems is the contamination and *spoofing* of the information on which nuclear-weapon-related decisions are based. Sensors and systems could be and have been fooled by either a false positive or a false negative. Hackers could also gain direct access to warning or communication systems and manipulate, contaminate, and corrupt information within these systems, leading to misunderstandings that could result in faulty decision-making in times of nuclear crisis. Finally, systems on board satellites are vulnerable to illicit access. The information on which nuclear systems and their operators rely is the most direct threat

vector, both in times of crisis and times of peace. Indeed, the mere **knowledge that sensitive nuclear systems could be compromised calls into question confidence in those systems**, regardless of the scale or nature of an attack.

The second challenge, which is not new, concerns **the risk of cyber disablement and destruction of nuclear weapons systems**. Cyber capabilities could be used to disable, disrupt or destroy these systems through malware, logic bombs, tampering with coding, or inserting Trojan horses into nuclear weapons software, systems or components. The supply chain is particularly vulnerable. According to a Chatham House report by Beyza Unal and Patricia Lewis, many aspects of nuclear weapons development, including warhead production and systems management, are privatized, and there is therefore a significant risk of vulnerabilities being introduced during manufacturing that compromise the overall integrity of national nuclear weapons systems.

4.2 Towards a third nuclear age and the end of the principle of "*deterrence*"

States' cyber capabilities are changing the composition of conventional and nuclear weapons systems, and challenging the principle of "*nuclear deterrence*".

While new technologies support system functionality, real-time decision-making and data processing, **new computers and complex codes also make systems less secure, more difficult to protect and therefore easier to compromise**. Increased reliance on increasingly complex information systems for nuclear operations increases the possibility of errors, failures and accidents. Similarly, the increasing use of commercial technologies creates significant risks. For example, several nuclear-weapon states rely on commercial technologies and components procured abroad for sensitive nuclear operations, because they are unable to manufacture high-tech components and computer chips.

The development of cyber capabilities also has a **transformative effect on other weapons systems**. The development of smart weapons, such as ballistic missile defences or satellite weapons, will have an impact on nuclear thinking and strategies. These new technologies may offer opportunities for "deterrence by denial": designed to intercept missiles or warheads after launch, they can also be used to prevent nuclear weapons systems from functioning as intended. This raises important questions for nuclear security, thinking and

strategy: the ability of states to target adversary targets vulnerable to missile shields, the role of advanced technologies as a non-nuclear counterforce, the risks of dual-use technologies, the use of artificial intelligence (AI), etc. While AI can assist in decision-making, the RAND Corporation points to its powerful destabilizing potential. **AI will strengthen the intelligence capabilities of the most advanced states, weakening "nuclear deterrence" and accelerating decision-making in nuclear crises.**

Thus, **the new cyber threat poses significant risks to the very principle of "*nuclear deterrence*"**. As a key element of future conflicts, offensive cyber capabilities, which give the advantage to the attacker rather than the defender, will increase tensions in times of crisis and could have important consequences for strategic stability, **requiring a radical rethinking of established nuclear concepts.**

The risks to nuclear command-and-control systems and to information and early warning systems could **render the nuclear order inoperative in a crisis**. In the case of both AI and cyber-attacks, the mere existence of such means of attack could undermine confidence in nuclear weapons systems and **call into question the nuclear second-strike capability**. Fear of losing the ability to retaliate **could make states feel so vulnerable that they might be tempted to take pre-emptive action.** These risks are heightened by the fact that several of the nuclear-weapon states maintain their nuclear forces on permanent alert, and launch times are becoming increasingly shorter. The development of offensive cyber capabilities could thus disrupt the traditional scale of escalation: states could be made vulnerable at any time by their enemies – state or non-state – and a "*permanent state of rivalry*" would be created.

According to Futter, these developments could have serious consequences for nuclear deterrence based on second-strike capability and the fear of mutually assured destruction. The potential use of cyber capabilities as precursors to delay or disrupt defensive systems before conducting a strategic attack introduces the risk that systems could be compromised and therefore not function as intended. **States would then reintroduce the possibility of pre-emptive strikes against nuclear weapons or associated systems.**

These cyber capabilities will also have **an impact on the likelihood of a future nuclear arms reduction agreement, as well as on nuclear proliferation**, because any arms reduction agreement could increase the influence of cyber threats. Cyber weapons thus represent a serious and growing counterforce risk and create a cyber security dilemma in terms

of which nuclear-weapon states must assume that their national security infrastructure has been targeted. This leads to a growing incentive for these states to adapt their nuclear policies towards "*preventive deterrence*" based on "*deterrence by denial*" rather than "*deterrence by punishment*". **The sanctity of nuclear norms is thus being entirely reassessed, raising fears of a lowering of the threshold for the use of nuclear weapons.**

4.3 Bibliography

- ARQUILLA, John, RONFELD, David, *Cyberwar is Coming*, RAND Corporation, 1993.

- BLAIR, Bruce, "Could U.S.-Russia Tensions Go Nuclear?" *Politico* (November 27, 2015), https://www.politico.com/magazine/story/2015/11/russia-us-tensions-nuclear-cold-war-213395/

- BORRIE, John, CAUGHLEY, Tim, WAN, Wilfred (eds), *Understanding Nuclear Weapon Risks*, UNIDIR, 2017.

- CIMBALA, Stephen J., "Nuclear Deterrence and Cyber: The Quest for Concept," *Air & Space Power Journal* (March-April 2014).

- CLECH, Jérôme, "Hybridity: New Threats, Strategic Inflection?" *Revue Défense Nationale*, vol. 3, no. 3 (2016), pp. 12-18, https://www.cairn.info/revue-defense-nationale-2016-3-page-12.htm

- DEJEAN, Philippe, SARTRE, Patrice, "La cyber-vulnérabilité," *Studies* (July-August 2015), pp. 21-31.

- DEPARTMENT OF DEFENSE OF THE UNITED STATES, DEFENSE SCIENCE BOARD, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, January 2013.

- DEPARTMENT OF DEFENSE OF THE UNITED STATES, *Nuclear Posture Review*, February 5, 2018.

- DOUZET, Frédérick, "Le cyberespace, un champ d'affrontement géopolitique," in GIBLIN, Béatrice (ed.), *Les conflits dans le monde: Approche géopolitique*, pp. 327-343, Armand Colin, Paris, 2016.

– DUNN, Will, "Can Nuclear Weapons Be Hacked?", *New Statesman* (May 7, 2018), https://www.newstatesman.com/spotlight-america/cyber/2018/05/can-nuclear-weapons-be-hacked

– FUTTER, Andrew, *Hacking the Bomb: Cyber Threats and Nuclear Weapons,* Georgetown University Press, Washington, DC, 2018.

– GEIST, Edward, LOHN, Andrew J., "How Might Artificial Intelligence Affect the Risk of Nuclear War?", *Security 2040*, RAND Corporation, 2018.

– GROLL, Elias, "How AI Could Destabilize Nuclear Deterrence," *Foreign Policy* (April 24, 2018), https://foreignpolicy.com/2018/04/24/how-ai-could-destabilize-nuclear-deterrence/

– HEALY, Jason, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," Issue Brief, Atlantic Council, Washington, DC, 2011.

– HOLLANDE, François, "Speech on Nuclear Deterrence," Istres (February 19, 2015).

– IASELLO, Emilio, "Is Cyber Deterrence an Illusory Course of Action?", *Journal of Strategic Security*, no. 1, Henley-Putnam University (2013).

– "Ile Longue. Les incroyables failles dans la sécurité," *Le Télégramme* (June 11, 2013), https://www.letelegramme.fr/ig/generales/fait-du-jour/ile-longue-des-failles-dans-la-securite-11-06-2013-2132250.php#7LdM2xQTcRHTzk4R.99

– MAZAAR, Michael J., "Rivalry's New Face," *Survival*, no. 54, vol. 4 (2012).

– FRENCH MINISTRY OF THE INTERIOR, MINISTERIAL DELEGATION FOR SECURITY INDUSTRIES AND THE FIGHT AGAINST CYBERMENACES, *State of the Digital Threat in 2017*, January 2017.

– NTI, The 2016 NTI Nuclear Security Index: Theft and Sabotage – Building a Framework for Assurance, Accountability, and Action, 3rd edition, January 2016.

– OFFICE OF THE PRESIDENT OF THE UNITED STATES, *International Strategy for Cyberspace*, 2011.

– PINTAT, Xavier, LORGEOUX, Jeanny, TRILLARD, André, ALLIZARD, Pascal, HAUT Claude, *La nécessaire modernisation de la dissuasion nucléaire*, Information Report no. 560 on behalf of the Senate Committee on Foreign Affairs, Defence and Armed Forces, May 23, 2017.

– SANGER, David E., BROAD William J., "Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms," *New York Times* (January 16, 2018), https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html

– STEWART, Phil, "Deep in the Pentagon, a Secret Program to Find Hidden Nuclear Missiles," Reuters (June 5, 2018), https://www.reuters.com/article/us-usa-pentagon-missiles-ai-insight-idUSKCN1J114J

– STOUTLAND, Page, "Growing Threat: Cyber and Nuclear Weapons Systems," *Bulletin of the Atomic Scientists* (October 18, 2017), https://thebulletin.org/2017/10/growing-threat-cyber-and-nuclear-weapons-systems/

– STOUTLAND, Page, PITTS-KIEFFER, Samantha, Nuclear Weapons in the Cyber Age: Report of the Cyber-Nuclear Weapons Study Group, NTI, September 2018.

– UNAL, Beyza, LEWIS, Patricia, *Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences*, International Security Department, Chatham House, January 2018.

– US HOUSE OF REPRESENTATIVES, The Report of the Select Committee on US National Security and Military/Commercial Concerns with the People's Republic of China, 1999.

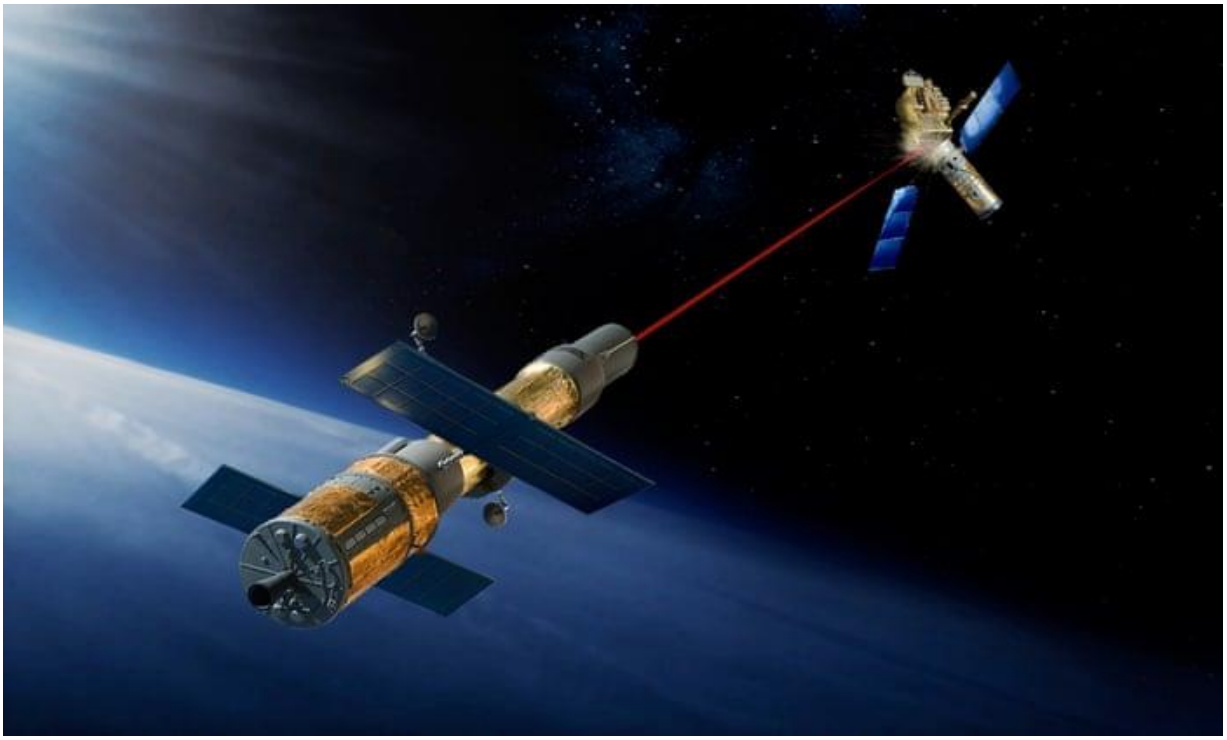
– VIZIER, Solène, *"SolarWinds: A Cyberattack that Challenges Nuclear Deterrence,"* IDN, January 2021, https://www.idn-france.org/nos-publications/actualites/solarwinds-cyberattaque-remet-en-cause-dissuasion-nucleaire/

– WIENER, Norbert, Cybernetics or Control and Communication in the Animal and the Machine, 2nd edition, M.I.T. Press, Cambridge, Mass., 1948.

5. THE SPACE WAR

Paul Quilès

Abstract: Space has become indispensable to economic and social life on Earth. But at the same time, it has become a new site of confrontation. Historically contained in the three domains of air, land and sea, strategic confrontation is extending to the cyber, space and cognitive fields. The exacerbation of international competition combined with the emergence of new technologies makes the prospect of a real space war – a new "star wars" – less and less hypothetical.



Reconstruction of a laser attack on a satellite.
Source: Erik Simonsen/Photographers Choice/Getty Images

In a recent interview with *Le Figaro*[5], General James Dickinson, commander of the US Space Command, said, "*Space will play a big role in the next conflict*", while General Michel Friedling, Commander of Space at the French Ministry of the Armed Forces, added, "*Space is a place of emerging threats*".

5.1 Some figures:

- 30 states have at least one satellite in orbit.
- There are 22,000 objects in orbit, including 2,000 operating satellites.
- Four hundred military satellites are in orbit, including 13 from France.
- There are three kinds of orbits: geostationary (36,000 km above the Earth's surface) for telecommunications satellites; low (between 160 and 2,000 km) for observation satellites (civil and military); and medium (between 2,000 and 35,786 km) for geolocation systems (GPS, Galileo).
- The Starlink project (SpaceX) plans to put 12,000 satellites into orbit.
- Seventy per cent of US intelligence comes from space.
- The US space budget is $50 billion and China's is $10 billion.
- According to Morgan Stanley, global space revenues are expected to grow from $350 billion today to $1 trillion in 2040.
- India, which has developed its first anti-satellite missile, and Japan are beginning to develop military space technologies and systems.

In short, space has become indispensable to our lives. In particular, the information on which all intellectual, commercial, cultural, social and healthcare activities are now based transits for a large part through space.

[5] *Le Figaro*, interview by Nicolas Barotte (July 2, 2021).

5.2 Can space be “regulated”?

Among other things, the 1967 UN Space Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies prohibits states from launching weapons of mass destruction into orbit. However, it does not prohibit the militarization of outer space or self-defence, and it does not define what is meant by the **peaceful use of outer space**.

At the UN and the Conference on Disarmament, China and Russia are proposing the non-deployment of weapons in space. In particular, Russia, through its foreign minister, Sergei Lavrov[6], has officially declared itself in favour of a legally binding international agreement against the deployment of weapons in space, but the United States rejects the idea because such a treaty would not include its rivals' ground-based anti-satellite weapons. Under these conditions, we are currently witnessing a veritable "weaponization" of space.

At the same time, discussions initiated by the European Union are under way between the United States, Britain, Canada, Australia, New Zealand and Germany to establish a **code of conduct** aimed at defining standards of responsible behaviour in space. This is the action most likely to provide credible and realistic responses to the dangers of a possible "space war".

5.3 Risks

In this new strategic and technological environment, all states, given their dependence on space systems and the vulnerability of these systems, but also the possibility of achieving supremacy in the context of geopolitical rivalry, are developing **defensive and offensive weapons** that make space a new field of conflict and the source of existential threats.

Russia has grasped the importance of this issue for re-establishing a strategic balance with the United States, and even more so has China, which, by developing a powerful space industry, directly threatens US hegemony.

[6] Declaration of 12 April 2021 on the occasion of the 60th anniversary of the flight of Yuri Gagarin.

5.3.1 Offensives weapons

China has been developing and testing a significant arsenal of **anti-satellite (ASAT) weapons** since the early 2000s, including:

- **Kinetic anti-satellite (KAS) capabilities** using surface- or air-launched missiles, but with the disadvantage that a kinetic strike against a low-orbiting satellite results in thousands of pieces of debris (currently 90% of objects in near space are debris);
- **Directed-energy weapons**, including ground-based lasers, anti-satellite missiles and anti-satellite orbital robots;
- Communications and GPS **signal-jamming satellites**; and
- **Spy satellites** and electronic and cyber systems to disable adversary space systems.

China is also preparing to launch its first **space-mining robot**. But China does not have a monopoly on offensive systems: the **United States** and all the "space" states such as **India** and **Japan**, for example, are also acquiring anti-satellite missiles and means of destroying or neutralizing the satellite systems on which most of the world's states depend.

5.3.2 Defensive weapons

The aim of defensive space weapons is to develop an "active defence" to ensure the preservation of space-based communications, navigation, observation, intelligence and targeting capabilities. The role of space will become even more vital when all combat systems are networked, and space will play a key role in the collection and distribution of real-time information.

Thus, the **United States** is developing a project for the gradual placing in orbit of a constellation of several hundred satellites whose role will be to instantly detect and transmit for targeting information on a threat of any kind whatsoever and at the same time to strengthen the resilience of its satellites in the event of anti-satellite attacks. The consequence of this project is the creation of a state of instant warfare that can only encourage the deployment of autonomous weapons systems.

As far as **France** is concerned, the behaviour in 2017 of the Russian satellite Luch-Olymp, which came a little too close to the Franco-Italian military communications satellite

Athena-Fidus, has made France aware of the vulnerability of its space capabilities. This is why it has undertaken the development of a Yoda space system (Eyes in Orbit for an Agile Demonstrator), a patrol satellite responsible for watching over French military satellites and a precursor to the development and deployment of jamming nanosatellites.

Space is also a transit point for the new hypervelocity intercontinental missiles.

5.4 Impact on "nuclear deterrence"

This ongoing "new space" revolution is opening up a new field of geopolitical competition within the framework of a power strategy that is no longer the prerogative of the traditional great powers alone.

The accelerated technological development of space systems offers new horizons in terms of data circulation and processing, but at the same time it increases the vulnerability of these systems. The strategy of nuclear terror, i.e. "nuclear deterrence", whose credibility now depends to a large extent on satellites for its command-and-control, observation, and navigation resources in particular, is becoming both useless and vulnerable, and therefore dangerous.

This conceptual and operational vulnerability is due to several factors:

- Firstly, the **civil-military** and **public-private duality** has become inherent to the space environment. The use of space is both a commercial and military issue; moreover, the technological building blocks used are dual purpose, which means that the civil and military dimensions of space-related technology are not always separate. This interweaving of the civil and military, the public and the private, has led to the uncontrolled emergence of **new** state and private **players** in this market, which is also becoming a forum for confrontation.

- This new dimension of space is now becoming a "grey" area where it becomes very **difficult to identify the perpetrator of unfriendly or hostile actions** conducted in space and to develop a proportionate response. Nuclear strategy is incompatible with this uncertainty about the ability to clearly identify an adversary. Conventional nuclear strategy cannot be exercised in this space "fog" and effectively becomes useless.

- **The dependence of nuclear strategy** on the growing role of space in the circulation and processing of data for its command networks and its intelligence and

observation capabilities, which are essential for the execution of nuclear strikes, **makes it extremely vulnerable** either to the neutralization of its space systems, rendering it inoperable, or to autonomous firing or pre-emptive firing for fear of an attack on its satellites, which have become highly vulnerable.

- The launching of thousands of satellites and swarms of nanosatellites, and their increasing role in the conduct of military operations, where speed and immediacy are becoming the determining factors, are giving rise to the concept of "**instant warfare**", i.e. the ability to start a war without any advanced warning or low alert signal. Instant war can be a substitute for the nuclear terror policy of deterrence, but it can also be a means of provoking a nuclear attack.

5.5 Conclusion

Space is now a site of military manoeuvre and confrontation, a structuring factor of power, and a real domain of strategic confrontation. More generally, it is an indispensable domain for all human activities. Thus, the neutralization of space systems in one form or another, whether selective or not, would have dramatic consequences for some or all of humanity without it being possible to clearly identify the origin of such a hostile act. This clearly indicates the importance of space strategy, which undermines the foundations of any nuclear strategy and renders it obsolete and useless.

However, at the same time, space strategy offers nuclear strategy the opportunity to become even more prominent and threatening.

A space strategy as part of a global conventional strategy therefore argues for the **abandonment of the nuclear strategy and the elimination of nuclear weapons**. But the very worrying prospects opened up by emerging technologies – in particular space technologies – also argue for the regulation and control of these new weapons systems, as has been done for the control of weapons of mass destruction.

5.6 Bibliography

- *Air & Cosmos*, "Military Space and Instant Warfare" (May 1, 2020).

- DUFFORT, Chloé, *Space, Armaments and Conflict: International Law in Orbit,* Open Diplomacy Institute (August 3, 2020), https://bit.ly/3xPgQ8J

- PASCO, Xavier, *"European Initiatives for Security in Space*, "Thucydides Centre, 2015, https://www.afri-ct.org/wp-content/uploads/2015/03/69-_Article_Pasco.pdf

- TESTE, Jean-Daniel, "La militarisation de l'espace: quels enjeux pour aujourd'hui et demain?", Areion24.news (April 8, 2021), https://www.areion24.news/2021/04/08/la-militarisation-de-lespace-quels-enjeux-pour-aujourdhui-et-demain/

6. ARTIFICIAL INTELLIGENCE

Bernard Norlain

Abstract: Artificial intelligence (AI) opens up revolutionary prospects in all fields of human activity. But if it is a multiplier of progress, it is also a multiplier of strength. As a result, it is becoming a priority defence issue for the competing powers of the 21st century. By its dual nature, AI favours the fusion of the civil and military and the appearance of new actors and uses. It plays an essential role in the battle to control and exploit information and allows for the robotization of decision-making and processes. Its impacts on nuclear strategy are therefore systemic, both because it makes this strategy obsolete and increases the risk of a nuclear conflict. Beyond that, AI and its applications constitute a real revolution for the conduct and control of future conflicts. A determining factor of military superiority, it is a real challenge to strategic stability.

Artistic representation of military applications of AI.
Source: K_E_N / Shutterstock

Vladimir Putin: "*Whoever becomes a leader in this field will be the master of the world.*"

6.1 Artificial intelligence: a strategic breakthrough

Defining AI is a difficult task, because the subject is so complex and has many forms. Schematically, AI aims to reproduce the human brain. It therefore refers to a programme with an ambitious objective: to understand how the human brain works and to reproduce it, i.e., to create cognitive processes comparable to those of human beings. The field is therefore extremely vast, both in terms of the technical procedures used and the disciplines involved, such as mathematics, computer science and cognitive science.

More concretely, AI is the result of the convergence between algorithms, the availability of large amounts of data, and progress in the accessibility of computing capacities. It reproduces cognitive processes by means of algorithms and the automated processing of "Big Data". Its current development is due to the rise of **machine learning**.

The French Atomic Energy and Alternative Energies Commission defines AI as *"a set of algorithms giving a machine the analytical and decision-making capabilities to adapt intelligently to situations by making predictions based on data already acquired"*. And Stuart Russell, a professor of Computer Science at the University of California, Berkeley, states that AI involves "*the study of how computers behave intelligently"*. The word "intelligence" would also need to be clarified at this point, but Yann Le Cun's lapidary definition ("*the ability to predict is the essence of intelligence*") is enough to characterize it.

AI is then a question of producing intelligent machines, which opens up revolutionary prospects at the scientific, technological, societal and human levels. Thus, for several years now, numerous publications have been describing the revolutionary prospects opened up by AI, and if, according to Elon Musk, AI is more dangerous than nuclear weapons, others are more optimistic, believing that the opportunities AI offers outweigh the risks. For the optimists, AI is the most powerful tool yet invented to benefit humanity, but all agree that AI in all its applications will disrupt our current way of life. In this respect, we could profitably repeat Thomas Edison's words about electricity: "*It is the field of fields. It contains the secrets that will reorganize the life of the world.*"

But if, to paraphrase Artur Rimbaud, AI is "*a multiplier of progress*", it is also becoming a "*multiplier of force*", and will therefore play a considerable role in future conflicts. AI technologies combined with advances in robotics, biotechnology and computer science are revolutionizing many fields, particularly defence. The range of defence-related AI applications is extremely wide, ranging from management applications to autonomous combat systems. In the field of defence and security, AI can be used to process masses of data for protection, observation and analysis functions, but it also enables automated decision-making, including for targeting and the use of lethal weapons.

The field of application is therefore vast, ranging from deep fakes to lethal drones. According to NATO's *Technology Trends Report 2020-2040*, "*the use of AI integrated with other associated technologies such as virtual or augmented reality, quantum computing, autonomy, modelling and simulation, space, materials research, logistics, data analysis, will have transformative effects on nuclear, aerospace, cyber, materials and biotechnology technologies".*

The report goes on to say that these transformations will be of the same order as "the introduction of nuclear weapons". **AI is now increasingly becoming a competitor to nuclear technologies and, paradoxically, while it makes nuclear deterrence increasingly useless, it simultaneously makes it increasingly dangerous**.

In our digital world, AI will accelerate the disruption that digitalization is already causing. It will therefore be one of the keys to the future of humankind, generating technological and strategic disruptions. Military doctrines will undergo profound changes caused by the rise of AI, and in the medium term, all military spaces will be occupied by more or less autonomous robotic units.

Thus, AI is becoming a **priority defence issue for the military powers of the 21st century**. But more than that, it is transforming politico-military dynamics and **changing the very nature of war**, and is thus taking on geostrategic importance. By allowing the emergence of new technologies at the point of origin of destabilizing weapons, it constitutes a real challenge to strategic stability.

6.2 The fields of AI

AI is intrinsic to the very many emerging technologies that are revolutionizing the art of warfare. These technological applications of AI, still immature in many ways, but whose development is characterized by its speed, present common aspects that can be grouped around three major poles.

6.2.1 Civilian-military, public-private duality

Currently, one of the major innovations in the field of defence technologies is that the civilian component is leading the military component: AI resulting from the convergence of calculation-algorithms-data is the best example. The technological building blocks needed to build weapons are no longer in the military domain, but in the civilian domain. We are thus witnessing a true civilian-military merger. The consequences are:

- A **public-private diversity of players**, especially in the field of research. The Google-Apple-Facebook-Amazon-Microsoft (GAFAM) and Baidu-Alibaba-Tencent-Xiaomi (BATX) groupings are investing tens of billions of dollars in AI research. But there is also a multiplication of other actors, both state and non-state, because any actor working in the AI field can create autonomous weapons. This diversity of actors automatically causes a proliferation of defence technologies;

- A **diversity of uses**, because civilian applications can be transposed to the military field. Moreover, new weapons systems such as hypervelocity missiles and hypersonic gliders, which can carry nuclear or conventional warheads and are therefore dual-use weapons, increase the risk of a nuclear pre-emptive strike in order to guarantee the response capability on which all nuclear deterrence depends.

Ultimately, this three-faceted duality (public-private, civilian-military, conventional-nuclear) contributes to the creation of a vast conflict arena in which technological, societal and state boundaries effectively dissolve and the "*fog of war*" dramatically increases.

6.2.2 The information war

The digital revolution has created a world based on information, and AI is the key information-processing tool. Information in a digital space becomes the essential value and its processing by AI allows all applications and manipulations to occur. The creation of false

information and fictitious but realistic faces, and the transformation on the fly of a voice by another are some of the applications that exemplify the information war in which the world is currently plunged and in which AI plays a primordial role. Observation, intelligence gathering, and command and control of combat operations, which are based on the gathering and analysis of information, are becoming a major field of AI application and are leading to the development of real-time digital combat strategies. Cyber space in both its offensive and defensive aspects is a huge field where AI can develop and introduce new opportunities: polyform computer viruses, the automation of cyber-attacks, the jamming of satellites, the usurpation of satellite data, etc. Combined in particular with quantum physics, **AI will prevent any cryptology system from being unbreakable**. On the other hand, however, because AI is a digital system, it will be susceptible to attack by other digital systems.

6.2.3 The robotization-autonomization of decisions and processes

Undoubtedly the question of autonomy, which lies at the heart of AI, is the most emblematic of its capabilities and challenges. If autonomy in its literal sense – i.e. the reproduction of the human brain – is still in the realm of utopia and science fiction, there is a continuum between what is autonomous and what is not, and there are therefore varying degrees or scales of autonomy. Thanks to deep learning, algorithms are opening up revolutionary perspectives such as the robotization of the battlefield and thus the removal of humans from lethal risk, but at the same time raise legal, ethical and strategic questions concerning the autonomous use of lethal force. In this area, **lethal autonomous weapons systems** (LAWS) carry the greatest symbolic weight. States are developing LAWS that, once activated, can select targets, track them and take some sort of violent action without human supervision. They are seen as military disruptors by being force multipliers: a small number of human controllers can operate swarms of weapons and drones in all environments. The development of LAWS in a context of an accelerating international arms race results in:

- A lowering of the threshold for armed conflict as a result of the increased use of robots that reduce the risk of human casualties, which previously inhibited conflict;
- An uncontrollable proliferation of LAWS;
- A clash of automated systems, leading to undesired conflict triggers;

– Automated decision-making, particularly in nuclear engagement, given the immediacy of the decisions that need to be taken in the case, for example, of the use of hypersonic missiles;

– Complete autonomy in the use of lethal force; and

– A facilitated violation of international humanitarian law, which requires, inter alia, the distinction to be maintained between authorized military targets and prohibited civilian or non-combatant targets and provides for criminal or disciplinary liability for those responsible for unlawful strikes.

Ultimately, the autonomy that AI offers will lead increasingly to the exclusion of humans from the military decision-making loop. This dangerous development is inherent to the development of emerging military technologies orchestrated by AI. The best human operator can do nothing in a conflict in which he/she is confronting multiple machines performing thousands of calculations and manoeuvres per second.

6.3 Impact of AI on "*nuclear deterrence*"

This quick and non-exhaustive review of AI applications inevitably leads one to question the concept of "*nuclear deterrence*" in this new strategic framework. Indeed, we note:

– An increase in the effectiveness of conventional armaments in terms of precision, robotization, speed of execution of operations and decisions, and the effectiveness of defensive missiles, which makes it possible to have a credible conventional deterrent;

– A duality that increases the "*fog of war*", which is incompatible with the clarity required by nuclear weapons and nuclear deterrence;

– A risk of the automation of the decision to deploy nuclear weapons;

– A conventional-nuclear duality of new weapons systems whose performance can provoke a pre-emptive nuclear strike because of the uncertainty of a second-strike capability;

– A revival of the nuclear arms race to restore this second-strike capability;

– High levels of vulnerability to cyber-attacks on nuclear weapon command-and-control systems;

- A decrease in the predictability of the threat analysis capability that makes the "*nuclear deterrent*" more vulnerable, but at the same time increases the risk of a pre-emptive strike;

- The revived proliferation of nuclear weapons; and

- A reduction in the inhibitions governing the use of nuclear weapons, thus lowering the threshold for nuclear weapons use.

Paradoxically, the consequences of the impact of AI applications on "*nuclear deterrence*" lead to the observation that it is being circumvented conventionally and is therefore useless, but simultaneously to the observation of an increase in the risk of nuclear conflict caused by an international arms race, the emergence of non-state actors, the automation of nuclear weapons-related systems, the increased vulnerability of these systems, and the risk of the misinterpretation and misperception of a perceived threat.

These observations lead one to argue for the abandonment of "*nuclear deterrence*" or, failing that, for the establishment of a global system of deterrence made up of a minimal "*nuclear deterrence*" and a strong conventional deterrence capability. However, the emergence of the disruptive technologies introduced by AI poses, beyond the questioning of the utility of "*nuclear deterrence*", the question of the need to reinvent a strategic stability that takes into account the new and often disturbing possibilities opened up by these scientific developments.

6.4 The war of the future

AI and its applications in new technologies, if they result in a new strategic landscape in which nuclear weapons are devalued, not to say rendered obsolete, are presaging a world in which the domains of conflict will not only be extended in quantitative terms into areas such as cyberspace and exo-atmospheric space, but also extended in qualitative terms by the new possibilities offered by these still-nascent scientific disciplines. To this extension of the field of combat is added a temporal dimension characterized by the acceleration of the rhythm of technological developments that dramatically increases the urgency of the need for a strategic reorganization.

Under these conditions, foresight becomes difficult, if not impossible, thus making the establishment of regulatory systems (the absolute necessity of which is already being felt) an improbable exercise. Nevertheless, based on current knowledge, we can imagine some characteristics of this new conflictual world:

- There will be a **blurring of traditional boundaries**, such as peace-war, civil-military, public-private, conventional-nuclear, friend-enemy, real-virtual, inside-outside, etc. The conflict space will become a blurred arena where conflict happens everywhere and nowhere. A new world will come into being in which traditional classifications and old concepts no longer apply. Strategic stability and international security must therefore be rethought in global terms.

- There will be an increasingly **strong presence of intelligent machines and neural networks**, which will result in the human being becoming distanced from action and decision-making – for good or ill – and the central issue will be that of preserving his/her role of controller and ultimate decision-maker.

- The **equalizing power of new technologies** will result in an increase in the number of state and non-state actors in the strategic arena, which in turn will lead to an even more complex, interconnected and interdependent world.

- There will be a **revolution in all forms of information**, whether it is false, real, virtual or augmented, which will make it a major strategic issue.

- A **"fog of war" will be created that considerably reduces the scope of the concept of coercion**, the use of brute force and particularly the use of nuclear force.

6.5 Conclusion

AI constitutes a real revolution in the conduct and control of future conflicts. It is becoming the key determining factor of military superiority and a real challenge to strategic stability. The first paradoxical consequence of the combination of new technologies and AI is that **it makes nuclear weapons obsolete, but at the same time increases the risk of a nuclear conflict**. This new situation argues, initially, for a rebalancing between "nuclear deterrence" and conventional deterrence, comprising a minimal form of nuclear deterrence and a system of conventional deterrence based on disruptive technologies. However, this new

strategic balance raises the key issue of the need to ensure that an uncontrolled arms race does not start and that strategic instability is not created in the long term.

6.6 Bibliography

- "Artificial Intelligence and Its Challenges for Defence," *National Defence Review*, no. 820 (May 2019), https://www.defnat.com/sommaires/sommaire.php?cidrevue=820
- CHAMAYOU, Grégoire, *Théorie du drone*, Ed. La Fabrique, April 2013.
- ERÄSTÖ, Tytti, *New Technologies and Nuclear Disarmament: Outlining a Way Forward*, SIPRI, May 2021, https://www.sipri.org/sites/default/files/202105/2105_new_technologies_and_nuclear_disarmament_0.pdf
- FAVARO, Marina, *Weapons of Mass Distortion: A New Approach to Emerging Technologies, Risk Reduction, and the Global Nuclear Order*, Centre for Science and Security Studies, King's College London, 2021.
- FUTTER, Andrew, *Explaining the Nuclear Challenges Posed by Emerging and Disruptive Technology: A Primer for European Policymakers and Professionals*, EU Non-Proliferation and Disarmament Consortium, March 2021, https://www.nonproliferation.eu/wp-content/uploads/2021/03/EUNPDC_no-73_FINAL-1.pdf
- KUBIAK, Katarzyna et al., *New Technologies, Complexity, Nuclear Decision Making and Arms Control: Workshop Report*, European Leadership Network (March 22-23, 2021), https://www.europeanleadershipnetwork.org/report/new-technologies-complexity-nuclear-decision-making-and-arms-control-workshop-report/
- LE CUN, Yann, *When the Machine Learns*, Ed. Odile Jacob, October 2019.
- NOËL, Jean-Christophe, "Artificial Intelligence: Towards a New Military Revolution?", *Strategic Focus (IFRI Studies)*, no. 84 (October 2018), https://www.ifri.org/fr/publications/etudes-de-lifri/focus-strategique/intelligence-artificielle-vers-une-nouvelle

- PATIRANA, P., "What Is Artificial Intelligence?", Medium.com (August 6, 2021), https://medium.com/@primeshs.17

- RUSSELL, Stuart, NORVIG, Peter, *Artificial Intelligence: A Modern Approach*, Pearson France, 2010.

- SHARKEY, Noel, "Algorithms Delegated with Life and Death Decisions," *National Defence Review*, no. 820 (May 2019), https://www.cairn.info/revue-defense-nationale-2019-5-page-173.htm?contenu=resume

- UK CABINET OFFICE, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, 2021, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

- USA, NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE, *Final Report*, 2021, https://www.nscai.gov/2021-final-report/

- VILLANI, Cédric, *Giving Meaning to Artificial Intelligence: For a National and European Strategy*, Parliamentary mission report, 2017-2018, https://www.vie-publique.fr/rapport/37225-donner-un-sens-lintelligence-artificielle-pour-une-strategie-nation

7. BIOTECHNOLOGY

Pablo Chaillat

Abstract: States have been attempting to regulate the military application of biological processes for over forty years. While biological weapons have long remained unusable or inaccessible, current technological innovations significantly enhance the applicability of biology in the context of warfare. Biotechnology has the potential to shape the face of modern warfare, making it less visible, more diffuse and more destructive. Collective consideration of these new dangers is required.

Biological weapons are considered weapons of mass destruction along with nuclear and chemical weapons
Source: Fastfission

7.1 Definitions and framing

Biotechnology is a field of science whose goal is the manipulation of biological processes through technology for industrial or medical purposes. Scientific advances in recent decades have led to a major development in our understanding of genetic and biological systems, while making it easier to manipulate them. The CRISPR (*Clustered Regularly Interspaced Short Palindromic Repeats*) technique, known as "*molecular scissors*", makes it possible to easily and rapidly modify the genomes of animal or plant cells. These scientific developments hold great promise for medical and industrial applications, through much more effective prevention and treatment of diseases, but they also raise ethical questions.

In addition, **genetic manipulation techniques have potential military applications**. A disease-carrying pathogen can thus be modified to increase its virulence, contagiousness or resistance to vaccines and other therapeutic interventions. Similarly, scientific progress makes it theoretically possible to create a new and destructive biological weapon, for example through:

- The development of synthetic (laboratory) pathogens that are already extinct or entirely new;
- From the modification of the immune system, the nervous system, the genome or the microbiome (microbiota genes);
- The use of gene drive systems to rapidly and economically disseminate harmful genes via animals or plants;
- The dissemination of pathogens and biological systems by new means.

Key trends in biotechnology and their implications for human safety

Key trends in biotechnology:

- Substantial investments are required, but once discoveries are made, they can be replicated almost immediately and at reduced cost.
- Access is facilitated to the knowledge, instruments and components needed to create living organisms.
- Hobbyists, self-taught scientists and other new players are entering the field of bioscience.
- The "toolbox" needed to manipulate genes and organisms (e.g. CRISPR) is evolving rapidly.
- There is a convergence between biology and other sciences and technologies (chemistry, engineering, computer science).
- Biological experiments, production and data are becoming increasingly digitized and automated.

Implications for human safety:

- New biological weapon;
- Increased potential for science to be hijacked by more actors;
- Increased potential for the misuse of science due to convergence with emerging technologies;
- Increased attack potential and vulnerabilities that can be exploited to cause damage;*
- An expanded grey area between legal defensive activities and illegal offensive activities; and
- Increased difficulty in detecting and attributing those responsible for a biological weapons attack.

* J. Kirkpatrick et al., Editing Biosecurity: Needs and Strategies for Governing Genome Editing, *Institute for Philosophy and Policy et al.*, December 2018

Source: F. Lentzos, "2019. Capturing Technology. Rethinking Arms Control", Conference, Berlin, March 15, 2019.

However, scientific advances in biology and the manipulation of genetic tissue are difficult to transfer to the military field in themselves. Therefore, **the fundamental revolution in the military application of biotechnology lies in the intersection of scientific advances in biology and the most recent technological developments in related fields**. Technological innovations in artificial intelligence (AI), (nano)robotics and 3D printing (or additive manufacturing), among others, make it possible to significantly increase the **applicability** of genetic manipulation techniques and organisms in the context of warfare. This results in the **need for ways to identify the predictability of a weapon and its effects on the adversary and, more broadly, on the balance of power.**

7.2 Biological weapons: a complicated development followed by international prohibition

Historically, the use of biological weapons has faced three major obstacles:

- First, the difficulty of controlling the effects of biological contagion and thus the risk of a **boomerang effect**;
- Secondly, to the **lack** of **precision and immediacy** of these weapons, the dispersion and dissemination of pathogens by air being very dependent on meteorological conditions on the one hand, and the contamination by the pathogen often taking several days and being rather random on the other hand;
- Finally, to the potential discovery of an **antidote or vaccine** by the adversary that would reverse the effects of the attack (biodefense).

Faced with these difficulties, almost all states have (officially) decided to renounce the development of biological weapons, a decision that was formalized by the entry into force in 1975 of the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (BWC), which **makes biological weapons illegal**.

Defining a biological weapon

In general, a biological weapon consists of a weaponized biological agent and a delivery system. Transforming an agent – i.e., selecting, designing, developing and manipulating it for specific, primarily military, purposes – is different from the simple use of biological materials, including pathogens or toxic agents, for hostile purposes. Weaponization seeks to ensure the effectiveness of a biological weapon by producing a suitable pathogen capable of infecting the target and causing disease or death by dissemination without being affected by environmental conditions or significantly attenuated by medical treatment or defensive measures.

The delivery system of a biological weapon is designed to facilitate the dissemination and dispersion of the agent in such a way as to render the target vulnerable to its effects. Examples of dissemination include the use of a spray tank on an aircraft to render an area inaccessible, the injection of an agent into a capsule or pellet, or the manual use of a targeted killing aerosol. In the case of aerosol dispersal, effectiveness depends on the agent's particle size being able to be absorbed by the target's respiratory system.

It is often more useful to examine biological weapon capabilities – i.e., whether a state is capable of threatening or launching a biological attack – than it is to know about the actual possession or stockpiling of such weapons. Distinguishing between an actor that possesses biological weapons and one that has access to military technology to develop a biological weapons programme is crucial to being able to assess risk and undertake control measures. These capabilities can be obtained not only through the implementation of an offensive military programme, but also through legitimate defence activities, life science research and the industrial development or formulation of biological agents. The processes and knowledge required for such activities are often difficult to distinguish.

*J.-P. Zanders, "Assessing the Risk of Chemical and Biological Weapons Proliferation to Terrorists", *Nonproliferation Review*, vol. 6, no. 4 (Autumn 1999), pp. 17-34, 18-19.

** E. Bohm et F. Lentzos, "Technical briefing note on developments in science and technology and governance in relation to biological weapons", *working paper*, SIPRI, November 2018.

7.3 At the crossroads of new technologies and biology

As many of the reports cited in this summary[7] point out, recent technological developments have made it much easier and more predictable to manipulate biological processes for military or terrorist purposes, thereby undermining the consensus on the ban on

[7] For an in-depth study, see in particular: BROCKMANN, Kolja et al, "Bio Plus X: Arms Control and the Convergence of Biology and Emerging Technologies", SIPRI, 2019

biological weapons. Above all, developments in the fields of 3D printing, AI and robotics are blurring the line between military and civilian applications, –making **these technologies inherently dual-use and therefore more difficult to control**.

7.3.1 3D printing (additive manufacturing) and biology

3D printing can be used, for example, to build on demand medical tools that are often needed in military fields, which is a positive development, but it can also facilitate the proliferation of weapons of mass destruction by circumventing state export controls on certain sensitive products. For example, **the use of 3D printing for the manufacture of armed drones could strengthen the capacity of certain non-state groups to launch a biological attack from the air, with precision and discretion**. Moreover, the digitization of 3D printing techniques makes them vulnerable to cyberattacks and thus to the theft of sensitive data. At the same time, the 3D printing of often highly sophisticated military parts requires a level of expertise that is beyond the reach of most non-state groups, thus reducing the risk of military proliferation.

7.3.2. Artificial intelligence and biology

AI, which aims to make robots more "*intelligent*" or "*autonomous*", in particular through the massive transmission of data extracted from the real world (*machine learning*), opens up new prospects for *human enhancement*. The use of *machine learning* for DNA analysis and genomic prediction could thus allow for a better identification of individuals receptive to human enhancement procedures, in particular through genomic manipulation. These advances are significant in the military field, since AI could make it possible to identify a soldier's needs at a given moment, to create personalized vaccines or drugs for each soldier according to his genetic heritage, or to increase the resistance of soldiers to a specific pathogen, or even to a biological weapon. However, AI developments are particularly worrying for the following reasons:

- AI could make it possible to discriminately target a group of individuals (based on certain genomic characteristics, exposure to a particular vaccine, or a specific vulnerability of their immune system), and thus opens the possibility of **"*surgical*" or even racist biological warfare**;

- AI could make it much easier to develop **advanced biological agents**, such as enhancing the **virulence** or **transmissibility** of a virus. However, these processes require

a high level of scientific sophistication, as well as a laboratory, and thus remain inaccessible to non-state actors, and extremely complex for states as well;

– The accumulation of data implied by AI increases the vulnerability of certain highly sensitive data to **cyberattacks** by a state or non-state group. This data could then be used to plan a "surgical" biological attack.

7.3.3 Robotics and biology

Through the automation of tasks, robotization allows for greater efficiency and reproducibility of scientific experiments, as well as increased productivity in the laboratory (robots can potentially reproduce experiments without interruption). Moreover, robotization also allows researchers to perform experiments remotely, by telling the machines what steps to perform. While robotics certainly offers promising prospects in a medical setting (prevention and rapid treatment of diseases, production and delivery of vaccines, etc.), it also has the potential to **make the development of biological weapons easier, faster and possibly accessible to a larger number of actors**. However, here again, the level of sophistication required for precision attacks is still beyond the reach of most non-state groups, and advances such as nanorobotics are still at an experimental stage.

7.3.4 Assessment of the risks arising from the convergence of new technologies and biology

– New technologies as a whole facilitate the development or production of biological weapons and their delivery systems.

– Moreover, they significantly increase the accuracy of biological weapons, undermining the consensus against their use.

– The increasing digitalization that accompanies new technologies increases the risk of cyber-attacks.

– Most new technologies are beyond the direct control of governments, which increases the potential for proliferation. Moreover, the high rate of technological innovation makes it more difficult to establish long-term technical parameters for export controls and transparency measures.

7.4 What are the consequences for "*nuclear deterrence*"?

As noted earlier, the effects of using biological weapons have traditionally been considered particularly random (lack of precision and immediacy) and even counterproductive (boomerang effect, discovery of an antidote by the adversary). As a result, biological weapons development programmes were largely abandoned by states and remained out of reach for non-state groups, which preferred more conservative methods. However, major advances in biotechnology in recent years, at the intersection of biology and new technologies, have provided solutions to most of these long-standing problems by increasing the ability of actors to control the effects of a biological attack –and thus increase the predictability of these weapons.

While this biotechnological '*new deal*' may not have a direct effect on nuclear weapons, other than to **further enhance the possibility of a nuclear *'first strike'*** in response to a biological attack, it may nevertheless encourage states to perceive biological weapons as a **new weapon of deterrence**. Advances in biotechnology make it theoretically possible for a state to infect a population in a targeted manner with a dormant virus, which could be activated at the desired moment. By playing up the psychological impact that such an announcement would have (panic of the population as a whole, chaos), a state could thus hope to apply a credible deterrence strategy.

More generally, **biotechnologies have the potential to shape the face of modern warfare, making it less visible, more diffuse and more destructive**. Above all, by weakening state control over strategic industries, **biotechnologies fuel a duality in their use that jeopardizes the non-proliferation framework as well as the doctrine of "nuclear deterrence", which is based on the identification of threats and the stability of the inter-state landscape**.

7.5 Conclusion

The issue of biological weapons control and prohibition has traditionally been approached from a biological perspective, and insufficiently from a technological perspective. Thus, most international treaties are not up to date with recent technological developments.

Significantly, the issue of duality, which is central to technological innovations and their intersection with biology, is largely absent from the 1972 Biological Weapons Convention (BWC), which focuses on the development of the weapons themselves.

These shortcomings are deeply worrying, because biotechnologies open the way to **new, more diffuse forms of deterrence, which it is important to grasp**. Therefore, and in view of the increasing complexity of the strategic landscape, would it not be wise to abandon the traditional nuclear deterrent, which appears obsolete?

7.6 Bibliography

- BEN OUARGHRAM-GORMLEY, "Gene Drives: The Good, the Bad, and the Hype," *Bulletin of the Atomic Scientists*, 2016, https://thebulletin.org/2016/10/gene-drives-the-good-the-bad-and-the-hype/

- BROCKMANN, Kolja et al, *Bio Plus X: Arms Control and the Convergence of Biology and Emerging Technologies*, SIPRI, 2019 https://www.sipri.org/publications/2019/other-publications/bio-plus-x-arms-control-and-convergence-biology-and-emerging-technologies

- CROSS, Glenn, "Wrestling with imponderables: assessing perceptions of biological-weapons utility", *The Nonproliferation Review*, 2021

- FEARS, Robin, TER MEULEN, Volker "Assessing the Security Implications of Genome Editing Technology: Report of an international workshop", *Frontiers in Bioengineering and Biotechnology,* Germany, 2017, https://www.interacademies.org/publication/assessing-security-implications-genome-editing-technology-report-international-workshop

- FINAUD Marc et al, *Global Biosecurity: Towards a New Governance Paradigm*, Slatkine, 2008.

- GALAMAS Francisco, "Biological Weapons, Nuclear Weapons and Deterrence: The Biotechnology Revolution", *Comparative Strategy*, 27:4, 2008, p 315-323.

- GALAMAS, Francisco, "Biotechnology and Biological Weapons: Challenges to the U.S. Regional Stability Strategy", *Comparative Strategy*, 2009, 28:2, 164-169, DOI: 10.1080/01495930902799756

- GALANOPOULO, L., "What ethics for genetic scissors?", *CNRS - The Journal*, 2016, https://lejournal.cnrs.fr/articles/quelle-ethique-pour-les-ciseaux-genetiques

- INTERACADEMY PARTNERSHIP, *The Biological and Toxin Weapons Convention: Implications of advances in science and technology,* 2015, https://www.interacademies.org/publication/biological-and-toxin-weapons-convention-implications-advances-science-and-technology

- KOBLENTZ, Gregory D, "The De Novo Synthesis of Horsepox Virus: Implications for Biosecurity and Recommendations for Preventing the Re-emergence of Smallpox," *Journal of Health Security*, Vol. 15, no. 6, 2018, pp. 620-28.

- KIRKPATRICK, Jessica et al, *Editing Biosecurity: Needs and Strategies for Governing Genome Editing*, George Mason University, 2018.

- LENTZOS, Filippa, "Ignore Bill Gates: Where Bioweapons Focus Really Belongs," *Bulletin of the Atomic Scientists*, 2017, https://thebulletin.org/2017/07/ignore-bill-gates-where-bioweapons-focus-really-belongs/

- LENTZOS, Filippa, INVERNIZZI, Cedric, "DNA Origami: unfolding risk?" *Bulletin of the Atomic Scientists*, 2018, https://thebulletin.org/2018/01/dna-origami-unfolding-risk/

- NATIONAL ACADEMIES OF SCIENCE, *Biodefense in the Age of Synthetic Biology* Washington DC, 2018.

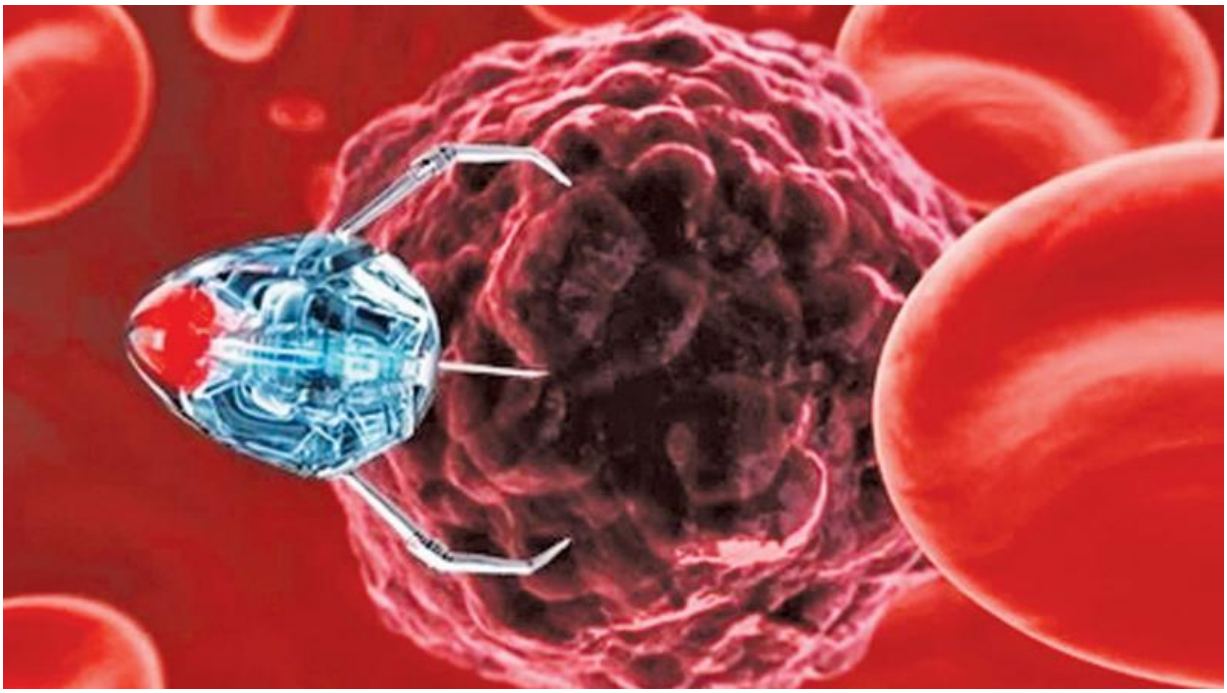
- ROYAL SOCIETY, "Trends In Synthetic Biology And Gain Of Function And Regulatory Implications," *Sackler Forum*, 2015, https://royalsociety.org/topics-policy/publications/2016/sackler-forum-report/

- THIBERGE, C., "Des insectes pour disséminer des virus, arme incontrôlable?", *Le Monde*, 2018, https://www.lemonde.fr/planete/article/2018/10/04/des-insectes-pour-disseminer-des-virus-une-arme-incontrolable_5364811_3244.html

8. NANOTECHNOLOGY

Anaïs Cren-Larvor

Abstract: By working on materials and electronics on a very small scale, nanotechnologies make it possible to miniaturize and disseminate highly sophisticated weapons, including nuclear weapons. Moreover, by offering unequalled detection capabilities, they can undermine any "nuclear deterrence" strategy, while increasing the risk of uncontrolled, accidental, or terrorist explosions.



Nanotechnology makes it possible to build nanobots that can both heal and kill.
Source: OnlyMyHealth

8.1 Description of nanotechnologies / nanosciences

8.1.1 What are nanotechnologies / nanosciences ?

Nanosciences are scientific studies that focus on the nanometric scale (10^{-9} m, or one billionth of a meter or one thousandth of a micrometer). Here we are almost at the atomic scale, with the size of a water molecule, for example, being of the order of 0.1 nanometer).

Nanotechnology is the study, fabrication and manipulation of material structures, devices and systems at scales of less than about 40 nanometers. Material structures can be tailored at extremely small scales to achieve specific properties. For example, materials can be made stronger, lighter, more durable, more reactive, or better electrical conductors, among other characteristics.

This is why nanotechnology is helping to significantly improve, if not revolutionize, many technological and industrial sectors: information technology, homeland security, medicine, transportation, energy, food safety, environmental science – and, unfortunately, weaponry, both conventional and nuclear.

Although the latter application area is rarely mentioned because of defence-related secrecy, it is clear that nanotechnology, which can lead to stronger, faster, and more portable systems that can handle and store ever-increasing amounts of information, is being heavily exploited by the military. There is a need for extremely robust and safe arming and triggering mechanisms for nuclear weapons, such as nuclear artillery shells. In these warheads, the nuclear explosive and its trigger undergo extreme acceleration, making it necessary that the essential components of the trigger be as strong and small as possible.

Nanotechnologies therefore have a very high destructive potential. But their dual nature (both civil and military) makes their regulation very complex.

8.1.2 What is the military impact of nanotechnology?

Nanotechnology allows users to:

- Store and analyse information more efficiently, thereby optimizing surveillance and intelligence information;
- Create better monitoring and detection devices (e.g. nanosensor swarms);

- Improve tactical decision-making (in conjunction with AI);
- Drastically improve existing weapons systems;
- Create "*smart*" weapons and ammunition and new weapons systems;
- Increase the autonomy of weapons systems; and
- Design and build systems that have an improved logistical and financial impact (stronger, cheaper vehicles, with extreme targeting accuracy; better profitability of production lines).

8.2 Impact of nanotechnology on nuclear weapons

Nanotechnology allows for a drastic improvement in nuclear weapons:

- It allows the creation of a fourth-generation micro-fusion nuclear bomb, resulting in:
    - A new system of slightly less powerful nuclear weapons (the equivalent of less than 1,000 tons of TNT) that blur the line between conventional weapons and weapons of mass destruction;
    - A very substantial increase in a state's firepower;
    - The creation of a so-called "clean" weapon with less radioactive fallout; and
    - The ability to bypass international monitoring systems, because the weapon does not actually cross the threshold for use as a nuclear weapon.
- It allows the creation of miniature nuclear weapons that:
    - Are more difficult to detect (or even invisible thanks to nanoscience);
    - Are triggered by a super-laser;
    - Are smaller, more manageable, and easier to transport and conceal;
    - Offer greater precision as a result of better information (obtained via nanocomputers); and

- are much more dangerous, because these mini-bombs could more easily be illicitly trafficked and end up in unexpected countries (or even in the hands of terrorist groups).

– It would lead to a rapid increase in nuclear arsenals through faster and cheaper manufacturing.

8.3 The impact of nanotechnology on nuclear strategy

A nuclear nano-armament could upset the global geostrategic balance in two ways:

– By offering a greater number of actors weapons that are out of all proportion to existing arsenals;

– By giving these actors unparalleled resistance capabilities in the face of attack risks of all kinds and from all sources.

Nanotechnology offers greater detection capability: a conventional nuclear warhead could be located much more quickly, and potentially destroyed or intercepted by hypersonic weapons that utilize nanotechnology.

In addition to nuclear weapons, nanotechnology allows the creation of new systems of autonomous weapons that are even more destructive than nuclear weapons, to the extent that a new term, "*nanotechnological deterrence*", has come into being:

– Very small systems with autonomous capacities close to those of living beings could acquire the capacity to reproduce, which would open the door to many new types of weapons.

– An attack (accidental, military or carried out by terrorists) of nanobots, molecular structures and other self-replicating pathogens could destroy the biomass and civilization in only a few days or weeks.

– The ability to replicate life at the molecular level may facilitate the development of new and more lethal biological weapons by independent actors.

A nanotechnology war would be extremely brief and destructive, destabilizing geostrategic balances, and threatening to transform the nuclear bomb from a weapon of "*deterrence*" to a weapon of employment.

A new balance of terror could emerge: it is possible that the nanotechnology arms race could lead to unbridled nuclear proliferation and the expansion of major nuclear arsenals to hundreds of thousands or even millions of warheads.

8.4 Geopolitical consequences

In a future nanotechnology conflict, if both (or more) sides are equipped with such weapons, the loss of life could run into millions. Because these weapons would be cheaper and easier to produce, the risk is that both states and non-state entities could acquire them. Such a development would call into question the current military and geopolitical balance among nations: the five nuclear-weapon states would no longer have the advantage, and their strategy of "*deterrence*" would collapse. Not only will this strategy be obsolete, but there is a risk of the pre-emptive use of nuclear weapons against a state that is developing nanotechnology weapons.

Nanotechnology thus threatens to undermine the power of "*nuclear deterrence*", so often invoked by the nuclear-weapon states, while increasing the risk of nuclear weapons being used. Here, as with other disruptive technologies, **a new international regulatory framework will have to be found that allows the continued development of nanotechnologies, but provides a much stronger framework to control their use in the military field.**

8.5 Bibliography

- DANIELS, Jeff, "Mini-nukes and Mosquito-like Robot Weapons Being Primed for Future Warfare," CNBC (March 17, 2017), https://www.cnbc.com/2017/03/17/mini-nukes-and-inspect-bot-weapons-being-primed-for-future-warfare.html

- FONDATION SCIENCES CITOYENNES, *Nanotechnologies and Military Applications* (February 5, 2011), https://sciencescitoyennes.org/wp-content/uploads/2012/12/nano-et-militaire.pdf

– Futura Tech, "After Nuclear Deterrence, Nanotechnology Deterrence?" (April 14, 2006), https://www.futura-sciences.com/tech/actualites/tech-apres-dissuasion-nucleaire-dissuasion-nanotechnologique-8657/

– GSPONER, André, "La nanotechnologie va permettre l'avènement d'armes nucléaires de quatrième génération," *Imagine Magazine* (September-October 2003), http://isri.ch/wiki/_media/publications:isri-03-07.pdf

– SANDBERG, Anders, BOSTROM, Nick, *Global Catastrophic Risks Survey*, Technical Report, Future of Humanity Institute, Oxford University, January 2008, pp. 1-5, https://www.fhi.ox.ac.uk/reports/2008-1.pdf

9. QUANTUM TECHNOLOGY

Pablo Chaillat

Abstract: Quantum technology promises to make current communication and location systems obsolete. The confidentiality and stealth imperatives at the heart of "nuclear deterrence" strategies will thus be profoundly undermined. By compressing time and space, quantum technology drastically increases the risk of nuclear escalation.

IBM Q System One quantum computer near Stuttgart.
Source: IBM

9.1 Definitions and framing

Physics is the science that tries to understand, model and explain the natural phenomena of the universe. For the man in the street, the understanding of "natural laws" is above all a work of observation of the world around us, like Isaac Newton supposedly discovering the law of gravity through watching an apple falling from a tree. However, this

common understanding, which is of the order of **"classical mechanics"**, does not apply to the atomic and subatomic domains of **"quantum mechanics"**, whose laws differ from, or even oppose, those of the world of solid, liquid and gaseous media that we can observe.

Two quantum phenomena (superposition and entanglement) present strong technological potential (quantum computers, communications, radar systems, sensors, etc.) with probable consequences for nuclear strategies.

9.2 Superposition, quantum computing and cryptology

The phenomenon of **superposition** works on the principle that in quantum mechanics, contrary to classical mechanics, elementary particles (protons, electrons, photons) are likely to be in *several states at the same time*. Indeed, in quantum mechanics an elementary particle can be defined with certain values, for example its speed, its position in space, and its rotation. At a given moment, if we prepare this elementary particle in a certain way, it can have several state values at the same time: for example, a photon could simultaneously be both upward and downward oriented.

9.2.1 Quantum computing

This quantum singularity opens up immense potential, particularly in **quantum computing** and the **ultra-fast processing of large amounts of data**. Unlike classical computers, where information is displayed as 0 or 1, quantum computers rely on **qubits** (quantum particles) that use superposition to adopt different states at the same time.[8] In other words, where a classical computer must process one possible solution after another to solve a complex problem, **a quantum computer can simultaneously and very rapidly search through all available information for common properties and detect a constant in the data**.

9.2.2 Quantum computing and cryptology

By enabling the rapid and efficient sorting of very large amounts of data, quantum computing promises to revolutionize sectors such as freight delivery (by calculating the best

[8] Some journal articles put forward the idea that the quantum computer opens the possibility of information being *both* 0 and 1 (0+1) and not only 0 *or* 1. However, the quantum phenomenon seems to be more complicated than this. We prefer the formulation "*different states at the same time*".

route), medicine (by understanding the origin of diseases and defining the best treatments based on a very large database of patients), and even financial and weather analysis. At the same time, the possibilities opened up by quantum computing also present certain risks, particularly in the field of **cryptology**. The most widely used current encryption systems work according to the RSA encryption method (named after its founders, Ronald Rivest, Adi Shamir and Leonard Adleman), which is based on the inability of a classical computer to explore every possible combination one after the other in an *acceptable time*. This operation is almost instantaneous for a classical computer in the case of a small number, but for a number with several tens or hundreds of digits, a classical computer could take years to find the solution, whereas the superposition system of the quantum computer allows it to perform the same operation in minutes or even seconds. However, nuclear codes are probably based on more complex combinations such as AES (Advanced Encryption Standard), which are currently quantum-resistant[9] – but perhaps not for much longer.

9.3 Intrication, cryptologie et capteurs quantiques

The phenomenon of **entanglement** is the second important characteristic of quantum mechanics that distinguishes it from classical mechanics. In the infinitely small realm, two particles can be linked by their state (i.e., *entangled*) regardless of the distance that separates them: a change in one of the particles will have an *immediate* effect on the state of the other particle.

9.3.1 Entanglement and communication systems

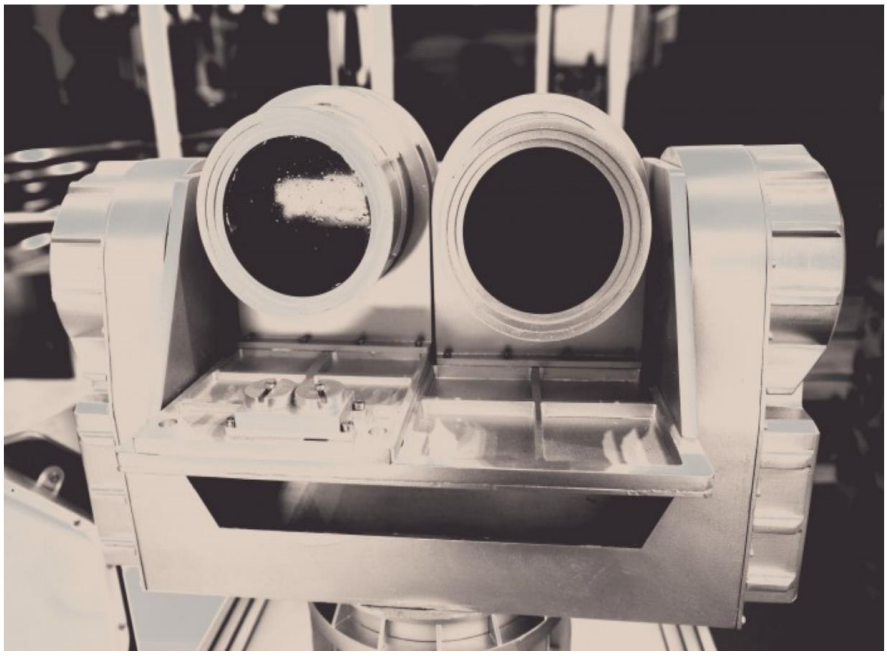
The technological applications of entanglement are immense, especially in communications and sensors. Quantum communication systems work through a machine that links two photons together (one is outside and the other remains inside the machine), thus creating a "*quantum key*", which is then *unbreakable* insofar as the intervention of an unauthorized actor on one part of the system would automatically have an effect on the whole system, according to the logic of entanglement, and would therefore be automatically

[9] Lane Wagner, "Is AES-256 Quantum Resistant?", qvault.io, September 10, 2020 (https://qvault.io/cryptography/is-aes-256-quantum-resistant/)..

detected. **Quantum communication thus makes nuclear weapons delivery systems much safer from the risks of cyber-attack**, as discussed in Chapter 4.

9.3.2 Quantum sensors: radars and gravimeters

The phenomenon of entanglement also holds great promise for improving quantum sensors, which can detect both stealth aircraft and nuclear submarines. In the case of a traditional radar, it works on a bouncing process: photons (or radio waves) are sent out into space, and when an aircraft is in that path, the relevant photons are sent back to the transmitter, revealing the position of the object being sought. This is why stealth aircraft are designed with a special shape and paint, allowing them to deflect these photons in all directions, and thus avoid their return to the transmitter. However, quantum sensors make this technology obsolete, since they work according to the phenomenon of entanglement: one photon is sent into space, while the other remains in the radar - the state of one influences the state of the other. So, if one photon is absorbed by the paint on a stealth aircraft, it will have a direct effect on the state of its entangled twin. **The phenomenon of entanglement thus makes it possible to develop high-performance radars capable of detecting stealthy objects to within a metre.**



Equipment of a prototype of quantum radar manufactured by China Electronics Technology Group
Source: Imaginechina via AP Images

In the case of submarines, it is the technology of gravimeters, highly improved in quantum version, which could make it possible to spy on their confidential trajectories. Indeed, if traditional gravimeters allow to evaluate the fluctuations of the terrestrial gravity according to the matter located under our feet, a quantum gravimeter could go as far as detecting underground movements of matter, to deduce the movements of stealthy objects.

9.1 Other applications: magnetometer, quantum compass and submarine detection

By using **magnetometers** traditionally used to measure magnetic anomalies, but augmented with quantum technology, it becomes possible a) to detect large metallic objects such as submarines, b) for these same submarines to navigate "by sight", or rather without the help of a conventional GPS, linked to a satellite. The "quantum compass" could allow nuclear submarines to no longer depend on conventional satellite communications, which are vulnerable to cyber attacks and make it more difficult to maintain stealth[10].

9.2 Consequences for "nuclear deterrence

The ability of quantum computing to break **computer codes** poses serious problems for "nuclear deterrence", particularly with regard to the confidentiality of nuclear codes or the location of nuclear bases or submarines. In a world where nuclear states are no longer able to keep the location of their launch sites secret, the incentive to strike first (knowing that one can hope to completely destroy one's opponent's nuclear response capability) would be greatly enhanced. Similarly, states could engage in massive rearmament, based on the logic that a multiplication of nuclear weapons makes it more difficult for an adversary to eliminate retaliatory capabilities with a single strike.

The potential consequences of **quantum sensors** for the strategy of "nuclear deterrence" are also immense, particularly with regard to the stealth requirement associated with the nuclear "triads" (air, ground, sea). To the extent that deterrence is based primarily on the *perceived* ability to inflict unacceptable harm in the event of an attack, these new

[10] Project Q, Peace & Security in a Quantum Age (https://projectqsydney.com/).

sensors could reduce decision-makers' confidence in their military ability to carry out a successful "second strike" in the absence of surprise. Conversely, as with cryptography, the inability to hide the location of nuclear submarines could provide an incentive for a state to strike first.

9.3 And France?

France is aware of the quantum race underway. Many countries, led by China, are investing massively in quantum research, in the hope of revolutionary technological applications. Europe has also invested heavily in quantum research and benefits from the prestige of its universities. The French Ministry of the Armed Forces has already planned to invest 30 million euros between 2019 and 2025 on research in quantum technology. For his part, President Macron has announced an overall investment of €1.8 billion from France. The Defence Innovation Agency (DIA) justifies its investment as follows: "*The exploration of such emerging technologies, and more broadly the early identification of potential breakthroughs, is the subject of exploratory research to prepare for the future beyond the 'foreseeable military need'*.

However, while the application of quantum mechanics offers interesting technological potential, it also increases the fragility of nuclear deterrence, which is based on the confidentiality of communication channels and nuclear launch sites. Moreover, by drastically shortening the response time to an attack, quantum technology may make a nuclear escalation scenario more likely than before. Research at the intersection of quantum technology and deterrence is still in its infancy, so the IDN report will certainly make an interesting contribution. **Project Q,** launched by Sydney University professor James Der Derian, seems to be the most promising initiative in this area today.

9.4 Bibliography

- DER DERIAN James & WENDT A., "'Quantizing international relations': The case for quantum approaches to international theory and security practice", *Security Dialogue*
- DER DERIAN, James, itw. par CASTRO Vic, "Drones, radars, nucléaires : comment le quantique va changer la guerre", *Numérama* (February 22, 2020),

https://www.numerama.com/politique/606950-drones-radars-nucleaire-comment-le-quantique-va-changer-la-guerre.html.

- DUFOUR, A., "Comprendre (un peu mieux) l'ordinateur quantique", *La Croix*, 2021, https://www.la-croix.com/JournalV2/Comprendre-peu-mieux-lordinateur-quantique-2021-05-04-1101153951

- GAMBERINI, S.J & RUBIN L., "Quantum Sensing's Potential Impacts on Strategic Deterrence and Modern Warfare", *Foreign Policy Research Institute,* 51(5), 399-413, 2021

- GILES Martin, "The US and China are in a quantum arms race that will transform warfare", *MIT Technology Review* (January 3, 2019), https://www.technologyreview.com/2019/01/03/137969/us-china-quantum-armsrace/#Echobox=1580145311

- HAYES Peter, "Nuclear Command and Control in the Quantum Era", *Nautilus*, (March 29, 2018), https://nautilus.org/napsnet/nuclear-command-and-control-in-the-quantum-era/

- KUBIAK Katarzyna, *Quantum Technology and Submarine Near-invulnerability*, European Leadership Network (December 11, 2020), https://www.europeanleadershipnetwork.org/policy-brief/quantum-technology-and-submarine-near-invulnerability/

- KUBIAK Katarzyna et al. "Nuclear Weapons Decision-making under Technological Complexity", European Leadership Network (March 25, 2021), https://www.europeanleadershipnetwork.org/policy-brief/quantum-technology-and-submarine-near-invulnerability/

- OWEN, T. & GORWA, R., "Quantum Leap: China's Satellite and the New Arm Race", *Foreign Affairs*, 2016

- ROBLIN, S, "No More 'Stealth' Submarines: Could Quantum 'Radar' Make Submarines Easy to Track (And Kill)?", *The National Interest*, 2019, https://nationalinterest.org/blog/buzz/no-more-stealth-submarines-could-quantum-radar-make-submarines-easy-track-and-kill-54547

- SOKOVA, Elena, *Disruptive Technologies and Nuclear Weapons*, Vienna Center for Disarmament and Non-Proliferation (July 17, 2020), https://vcdnp.org/disruptive-technologies-and-nuclear-weapons/.

- WADHWA, Vivek, "Quantum Computers may be more of an imminent threat than AI", *The Washington Post*, 2018, https://www.washingtonpost.com/news/innovations/wp/2018/02/05/quantum-computers-may-be-more-of-an-imminent-threat-than-ai/

10. CONCLUSIONS

Abstract: At a time when the nuclear threat is already hanging over humanity, new technologies are emerging that will in the short term both increase the risk of nuclear catastrophe and render obsolete the strategy of nuclear deterrence, which has already been condemned internationally as illegal. This is what this study has attempted to demonstrate..

French nuclear test in Polynesia in 1971
Source: CTBTO Image Bank

The so-called "*nuclear deterrence*" strategy adopted by France consists of threatening any state that attacks its "vital interests" with "absolutely unacceptable damage to its centres of power, i.e. its political, economic and military nerve centres".[11] It cannot be said often enough that this strategy is contrary to international law, which requires, in particular, that

[11] Speech by President Emmanuel Macron to the Ecole de Guerre (February 7, 2020).

actions taken in self-defence should be necessary and proportionate and that civilians should be spared, failing which it amounts to a war crime or even a crime against humanity, and that nuclear disarmament be negotiated "*in good faith*". This is why the French authorities no longer refer to the consequences of this strategy: they no longer speak of an "*anti-cities strategy*" and assert, without any possible certainty, that the destructive power of nuclear force will dissuade the aggressor from attacking France and thus avoid war.

The very term "*dissuasion*", which the French use to translate the English term "*deterrence*", is a euphemism chosen on purpose by the designers of the French doctrine. It implies a rational calculation on the part of the adversary, which is by no means guaranteed. It is semantically distinct from the English term "*deterrence*", whose root is the same as "*terror*" or "*terrorism*". More honestly, the other nuclear powers admit that their goal is to strike terror into potential adversaries, but also into their populations. But the strategy is basically the same. It is in fact all of humanity that is being blackmailed, given the global humanitarian consequences of any nuclear war, even a regional one.

This **ability to terrorize populations** is obviously based on a technology, the nuclear explosion, the effects of which were demonstrated in Hiroshima and Nagasaki, but also by some 2,121 nuclear tests, 520 of which were in the atmosphere (the equivalent of 29,000 Hiroshima bombs). This technology was discovered more than 80 years ago, and it was to prevent Hitler from acquiring the atomic bomb that the United States launched the colossal Manhattan Project in 1942. Despite the developments and modernizations that have taken place since then, the technology remains almost identical to that used in the Hiroshima and Nagasaki bombs.

At the same time, the world has seen the emergence of **new technologies that make the nuclear threat strategy vulnerable and ultimately obsolete**. Proponents of nuclear weapons respond to those who seek to eliminate them by saying that they cannot be "dis-invented". But history is replete with technologies, including defence technologies, that have been overtaken by new discoveries and abandoned, ranging from the bow and arrow to the sailing ship.

Thus, **artificial intelligence (AI)**, so fascinating for everyone, also appeals to the military, which is concerned about limiting the loss of personnel in combat and is interested in **autonomous weapons systems** or unmanned aircraft. Introducing such autonomy in command-and-control systems for nuclear weapons would no longer make it possible to avoid

the false alarms detected by humans, thanks to whom the world has escaped disaster several times.

The nuclear threat strategy is based on the ability to respond to a first strike, mainly by means of missiles fired from supposedly undetectable and therefore invulnerable submarines. However, the combined progress of **AI** and **quantum computing** will sooner or later make it possible to calculate the trajectories of submarines and thus to target them just as easily as air bases or land-based missile silos. This is a sobering thought, given the assurance of the French minister of the armed forces, who recently stated that third-generation French ballistic missile submarines would sail until 2090!

Digital capabilities combined with **AI** could just as easily hack the authentication and authorization systems used to approve the launch of nuclear weapons once a threat is detected. For example, **deep fake** technology could be used to mimic a communication or video recording from the leader confirming his or her approval of the launch, resulting in an inadvertent attack.

Offensive and defensive (anti-missile) nuclear systems also depend on encrypted communications networks deployed on orbiting satellites. However, the encryption of these networks has become vulnerable to **quantum-computing-enhanced cyber-attacks**, and the satellites themselves can easily be attacked by seemingly accidental **kinetic collisions** or **directed-energy weapons** (e.g., powerful lasers). Cyber-attacks, which in themselves are almost impossible to attribute to a specific opponent, could also focus on command-and-control centres and either disable detection or launch systems or cause unauthorized missile launches that could result in a nuclear response.

Hypervelocity technology **(hypersonic missiles)** has also become attractive to those nuclear powers that fear a decapitating first strike and are further encouraged by anti-missile systems capable of repelling any retaliation. By investing heavily in missiles that are faster and, above all, more manoeuvrable than ballistic or even cruise missiles, these nuclear powers will be encouraged to carry out pre-emptive strikes and thus contribute to lowering the threshold for the use of nuclear weapons. Nuclear weapons have thus gone from being a deterrent to becoming a combat weapon without any realistic restraint on their use.

Another technology is already linked to the nuclear threat, that of the **electromagnetic pulse**, which is capable, by using nuclear weapons or combined with

microwave or hyperfrequency weapons, of creating strategic chaos caused by the interruption of communications, computer systems and electricity distribution, the paralysis of command-and-control systems, and the resultant inability to control military forces. This scenario is that of the "final warning" foreseen by France in case of the failure of deterrence (which is thus admitted as a possibility) and likely to trigger nuclear escalation. The nuclear threshold would be crossed and, moreover, it would be impossible to target only military objectives, because all critical infrastructure (air traffic control, hospitals, civilian nuclear power plants, banking systems, etc.) would potentially be paralyzed.

Eventually, even if this still sounds like science fiction, one can imagine **nanobots** saturating command-and-control systems or any military infrastructure apparently protected against kinetic attacks and wiping out any offensive or defensive capacity. And closer to home, what about the ability of AI-equipped drones to penetrate even sophisticated protective domes such as the Israeli Patriot system?

Thus, the risks posed by these new technologies to the nuclear threat strategy can only increase the likelihood of nuclear detonations, whether by mistake, accident or terrorist action. This in itself should be enough to convince the leaders of the nuclear-armed powers to abandon this strategy, which has become unacceptably dangerous.

Moreover, **these new technologies could in the short term render the so-called "*nuclear deterrent*" completely obsolete and ineffective** – which is all the more reason to put an end to them, while ensuring that the potential offered by these new technologies, in particular autonomous weapons and cyber attacks, is not worse than the evil system of nuclear deterrence, i.e. does not further threaten sensitive infrastructure or civilian populations. There is therefore a great deal of work ahead for diplomats, lawyers, military experts and civil society, especially since, while nuclear weapons are still in the hands of states, cyber weapons are much more likely to fall into the hands of criminal or terrorist groups that are more difficult to control or reach, or even impossible to bring to a negotiating table.

10.1 Bibliography

– BRUSTLEIN, Corentin, "Strategic Risk Reduction among Nuclear Powers," Proliferation Papers (IFRI), no. 63 (January 2021),

https://www.ifri.org/sites/default/files/atoms/files/brustlein_risk_reduction_nuclear_weapons_possessors_2021.pdf

- ERÄSTÖ, Tytti, *New Technologies and Nuclear Disarmament*, SIPRI (May 7, 2021), https://www.sipri.org/publications/2021/other-publications/new-technologies-and-nuclear-disarmament-outlining-way-forward

- FAVARO, Marina, "Emerging Technologies and Nuclear Stability," European Leadership Network (July 19, 2021), https://www.europeanleadershipnetwork.org/commentary/emerging-technologies-and-nuclear-stability/

- GNESOTTO, Nicole, "Technological Revolutions: For Better or for War?", Normandy World Peace Forum (2019), https://normandiepourlapaix.fr/ressources/nicole-gnesotto-revolutions-technologiques-pour-le-meilleur-ou-pour-la-guerre

- JOHNSON, James, KRABILL, Eleanor, "AI, Cyberspace and Nuclear Weapons," War on the Rocks (January 31, 2020), https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons/

- MAITRE, Emmanuelle, "Phébé – La dissuasion nucléaire à l'épreuve de la technologie," *Le Point* (July 3, 2018), https://www.lepoint.fr/phebe/phebe-ces-technologies-qui-menacent-la-dissuasion-nucleaire-03-07-2018-2232655_3590.php

- SEIBT, Sebastien, "From the A-Bomb to the AI-Bomb," France 24 (May 9, 2019), https://www.france24.com/fr/20190509-ia-intelligence-artificielle-nucleaire-menace-atomique-sipri-russie

- SU, Fei et al., *Artificial Intelligence, Strategic Stability and Nuclear Risk*, SIPRI (June 2020), https://www.sipri.org/publications/2020/other-publications/artificial-intelligence-strategic-stability-and-nuclear-risk

ABOUT THE AUTHORS

ACKNOWLEDGEMENTS

ANAÏS CREN-LARVOR

Anaïs Cren-Larvor holds a master's degree in International Public Law and specializes in the non-proliferation of nuclear weapons and the physical protection of nuclear materials and facilities.

She completed an internship at IDN and is currently an international cooperation project manager at Astove Conseil.

BERNARD NORLAIN

Président d'IDN

Air Force General (2S) and IDN President since October 2021, Bernard Norlain is a graduate of the Ecole de l'Air and a former fighter pilot. He served as chief of the Military Cabinet of prime ministers Jacques Chirac and Michel Rocard.

He directed the Institut des Hautes Etudes de Défense Nationale (1994-1996), was vice-chairman of Deloitte & Touche France, and then chairman and CEO of SOFEMA Group. He is currently honorary chairman of the Study Committee of the Revue Défense Nationale. He is a Commander of the Legion of Honour and has received the Mahatma Gandhi Gold Medal from UNESCO. For IDN, he is in charge of the External Relations Department. He is co-author of Stop the Bomb! (2013) with Paul Quilès and Jean-Marie-Collin.

JACQUES FATH

IDN board member

Member of the IDN board since October 2021, Jacques Fath is an independent researcher, specialist in international relations, security and peace issues. His approach is resolutely critical of the policies and currents of thought that are dominant in the media today.

He is a graduate of the Institut d'Études Politiques (Grenoble) and holds a degree in sociology. He is the author of: "Penser l'après… Essai sur la sécurité, la puissance et la paix dans le nouvel état du monde " (2015), "Terrorisme. Réalités, causes et mystifications idéologiques" (2019) and "Chaos. La crise de l'ordre international libéral. La France et l'Europe dans l'ordre américain" (2020).

MARC FINAUD

IDN Vice President

A former career diplomat, Marc Finaud works as a trainer for young diplomats and officers at the Geneva Centre for Security Policy (GCSP) in all areas of international security. During his diplomatic career, he was assigned to several bilateral posts (USSR, Poland, Israel, Australia) as well as to multilateral missions (CSCE, Conference on Disarmament, UN), and was a Scientific Collaborator of the United Nations Institute for Disarmament Research (UNIDIR) (Weapons of Mass Destruction Program).

As Vice President of IDN, he is responsible for the association's international and diplomatic relations. He is the author of "L'arme nucléaire : éliminons-la avant qu'elle nous élimine" (2020).

PABLO CHAILLAT

IDN board member

Pablo Chaillat holds a master's degree in International Security from the University of Warwick (UK). He also holds a double degree in History and Philosophy, obtained during three years of preparatory classes for the Grandes Ecoles in Paris.

He works as a junior professional officer at the Geneva Centre for Security Policy. Passionate about conflict prevention and peace building, he specializes in the geopolitics of the Near and Middle East. He contributes to the Research and External Relations divisions.

PAUL QUILÈS

Former President of IDN

Recently deceased, Paul Quilès held several elected and ministerial positions. Minister of Defense, he was also vice-president of the Defense and Armed Forces Committee of the National Assembly. A former mayor of Cordes sur Ciel (Tarn), he has long been involved in the fight for nuclear disarmament.

As founding member of IDN, he was its president until his death. He was the author of "Face aux désordres du monde" (2006), "Nucléaire, un mensonge français" (2012), "L'Illusion nucléaire avec" (2012) and "Arrêtez la bombe!" (2013).

SOLÈNE VIZIER

IDN board member

Passionate about geopolitics, Solène Vizier holds a double Master's degree in Strategic Studies from the University of Paris 13 and in Cybersecurity, Cyberterrorism and Cyberwarfare from the INISEG (Spain). She currently works as an analyst in a firm specialized in digital strategy.

She is a member of the Cyber working group of the EGA Institute. Within IDN, she is in charge of the Research Unit.

Thanks to **Annick Suzor-Weiner**, vice-president of IDN and Pugwash France, **Blaise Imbert**, IDN treasurer, **Thierry Lorho**, designer of the Mileva artificial intelligence system, and **Félix Anthonysamy**, trainee, for their kind and substantial contributions.

Cover design: **Félix Anthonysamy** © IDN 2021.