Toda Peace Institute

Policy Brief No. 89 September 2020

Technology, Arms Control and World Order:
Fundamental Change Needed

Jürgen Altmann

1. Introduction: Military-Technological Revolutions

Over centuries, advances in science and technology have made possible new kinds of weapons that often provided an advantage in war. Changes in the technology of war mostly occur gradually, but sometimes qualitative change is so big that one can speak of military-technological revolutions. One is marked by the introduction of firearms; another was brought about by nuclear weapons. For about thirty years, the term "revolution in military affairs" has been used for the rise of electronics, sensors, precision weapons, networked communication, combined to a "system of systems". Now we are on the verge of a more fundamental revolution, characterised by cyber warfare, autonomous weapon systems, general military use of artificial intelligence, with new possibilities in the fields of genetics, of manipulation of the human body and mind, and more wide-spread access to technologies of destruction.[1]

---

[1] This text builds on Jürgen Altmann (2020), New Military Technologies: Dangers for International Security and Peace, Sicherheit & Frieden/Security and Peace, 38 (1), 36-42. See there for more references.

2. Qualitative Arms Race and Predominance of the USA

After the end of the Cold War, military spending decreased significantly at first, but spending for military research and development (R&D) continued with only little reduction and soon increased again.[2] At present, the USA spends around $70 billion per year for military R&D, 10% of its total military expenditure.[3] Russia's expenditure is $4-5 billion, around 8% of the military total.[4] The UK and France spend $2.4 billion and $1.3 billion (4.9 and 2.4%), respectively.[5] For China, no R&D budget figures are available. Speculating that China spends 5-10% of its total military expenditure for R&D, one gets $13 - $25 billion, one sixth to one third of the US figure.[6]

While the share of the USA in total global military spending is about 38%, in military R&D its portion is nearly two thirds of the global total. The depth and width of its efforts are unrivalled, making the USA the leader in new military technologies. This is a consequence of the permanent goal of maintaining military-technological superiority, which fuels arms races and creates serious problems for international security (see Section 6). Since the USA is most advanced, one generally can learn about actual and potential trends by looking at the US R&D activities, information about which is available to a high degree.

Other countries are investing in new military technologies, too. For example, France has set guidelines for developing artificial intelligence for defence, India has tested an anti-satellite weapon, Israel is a leader in uninhabited air vehicles. Countries without big military R&D operations can get access by importing new weapons and other systems. Arms races and shortened decision times will also occur on regional levels. Nevertheless, the pace of qualitative advance is determined by the USA, Russia and China.

---

[2] Altmann, Jürgen (2017). Militärische Forschung und Entwicklung (Military Research and Development). In Jürgen Altmann, Ute Bernhardt, Kathryn Nixdorff, Ingo Ruhmann und Dieter Wöhrle. *Naturwissenschaft – Rüstung – Frieden – Basiswissen für die Friedensforschung (Science – Armament – Peace – Basic Knowledge for Peace Research)*. 2nd edition. Wiesbaden: Springer VS.

[3] US military R&D expenditure 2018: $67.5 b (in constant 2018-$), computed from Tables 57 and 58 in Main Science and Technology Indicators, Volume 2019, Issue 2, OECD, 06 Mar 2020, https://www.oecd-ilibrary.org/docserver/g2g9ff07-en.pdf 25 May 2020); US total defence expenditure 2018: $682.5 billion (in constant 2018-$), SIPRI Military Expenditure Database, https://www.sipri.org/sites/default/files/SIPRI-Milex-data-1949-2019.xlsx (7 May 2020).

[4] RBL 325 billion for "Applied R&D in field of National Defence" and RBL 3,850 billion total military expenditure (Julian Cooper, Russian military expenditure in 2017 and 2018, arms procurement and prospects for 2019 and beyond, University of Oxford, February 2019, http://www.ccw.ox.ac.uk/s/Russian-military-expenditure-in-2017-and-2018-by-Cooper.pdf (26 May 2020)). The first figure, with an exchange rate of 60-70 RBL/$, gives $ 4-5 billion. Note that the total military expenditure of Russia, $61.4 b, ranks fifth after the USA ($683b), China ($253b), Saudi Arabia ($74b) and India ($66b). On ranks 6 to 10 are: France ($51b), UK ($50b), Japan ($47b), Germany ($47b) and South Korea ($43b). Then there is an expenditure gap to rank 11 (Brazil with $28b). (2018 figures in 2018-$, China and Saudi Arabia estimated, SIPRI 2020 (op. cit.)).

[5] 2018, computed from Tables 57 and 58 in OECD 2020 (op.cit.) with total military expenditures of $49.9b (UK) and $51.4b (France) in SIPRI 2020 (op.cit.).

[6] Total expenditure: $253b (note 4).

3. Preventive Arms Control[7]

One task of natural-science/technical peace research is assessing potential military applications of new technologies. Could they create problems for arms control, for disarmament, or for international humanitarian law? Could they stimulate an arms race or destabilise the situation between potential adversaries? Could they cause problems for humans, the environment or society even outside of war? To prevent such dangers, science has developed concepts for preventive limitations in many areas. There have been proposals for bans on ballistic missile defence, on space weapons, on high-energy laser weapons, on tests of hypersonic missiles, on autonomous weapon systems. In several cases states have taken up such proposals or developed them by themselves, sometimes after quite long times. Preventive elements are included e.g. in the nuclear testing treaties, the ABM Treaty (now defunct), the Biological and Chemical Weapons Conventions. But general advance in military technologies was not slowed down, probably because in the face of perceived threats states found their own military strength more important than co-operatively organising international security in a better way.[8]

Preventive arms control pursues the classical goals of arms control, with war prevention the highest priority; it is directed at potential future deployments. Dangers from them could be contained with sufficient insight and political will. Successes in excluding not yet existing military systems could prepare the ground for reductions in existing armaments. The associated reductions of tensions could also contribute to more comprehensive global governance concerning the risks of civilian uses of new technologies.[9]

4. Fields in Present Military R&D

Some fields of military R&D are continuations of activities started in the Cold War, such as space weapons, ballistic missile defence and hypersonic missiles. Others have appeared only in the last two decades, e.g. cyber weapons or artificial intelligence. On the one hand, work is being done for concrete military systems; on the other hand, generic technologies are being studied that may have many different military applications. The generic technologies also stimulate each other.

---

[7] Wim Smit, John Grin and Lev Voronkov (eds.) (1992), Military Technological Innovation and Stability in a Changing World – Politically assessing and influencing weapon innovation and military research and development. Amsterdam: VU University Press; Jürgen Altmann (2006), Military Nanotechnology - Potential Applications and Preventive Arms Control, Abingdon/New York: Routledge: ch. 5.

[8] The end of the Cold War and the decade after it shows how such a co-operative process can start, with a fast sequence of important arms-control treaties: 1987 INF Treaty, 1990 CFE Treaty, 1992 Open Skies Treaty, 1993 Chemical Weapons Convention, 1991/93/97 START, 1996 CTBT). Unfortunately, for several reasons, that period full of hopes came to an early end.

[9] On both aspects see e.g. Thomas G. Weiss and Ramesh Thakur (2010), Global Governance and the UN: An Unfinished Journey, Bloomington: Indiana University Press, 2010.

Ballistic Missile Defence[10]

Following the ABM Treaty (1972), the USSR had kept one ABM system while the USA had deactivated its ABM bases. In the 1980s the US Strategic Defense Initiative (SDI) brought ideas of full protection against nuclear warheads by space-based beam weapons, but they turned out to be unrealistic. In the 1990s, US interest in ballistic missile defence (BMD) grew again, with an extensive development and testing programme. After abrogating the ABM Treaty (2001/2002), the USA deployed BMD systems in several regions at sea and on land. The interceptors are to hit the incoming reentry vehicles in midcourse while they fall through space along the gravity-caused ellipse. Slower ballistic missiles of shorter ranges are to be hit by other interceptors in the terminal phase. Even though midcourse defence against missiles with decoys is questionable, Russia and China are working on hypersonic glide vehicles in order to circumvent US BMD sites.

Whereas the present BMD systems are directed against limited attacks e.g. from North Korea, the Trump administration has expanded the scope to any missile launched against the USA, including from Russia and China. Here hypersonic glide vehicles will pose particular difficulties.

Space Weapons[11,12]

Soon after the first satellites, efforts for anti-satellite (ASAT) weapons began. In the 1960s and 1970s the USSR developed and tested rendezvous/follower satellites for attack by shrapnel. In the 1980s the USA developed and tested direct-ascent, direct-hit ASAT systems. Directed-energy weapons for destroying the nuclear warheads of ballistic missiles, promoted under the US SDI, would have had much higher capabilities against satellites, but these concepts were put to rest. Later the USA deployed ballistic-missile defence missiles with a hit-to-kill vehicle. Using one of these, the US destroyed one of its satellites in 2006. Russia has been developing a direct-ascent system since the 2000s; test flights have not been destructive. In 2007, China hit one of its satellites using similar technology. India followed with a destructive ASAT test in 2019.

Satellites are of central importance for military operations, creating incentives for ASAT weapons. However, the debris created from tests endangers many other satellites. Depending on the satellite orbit and the ASAT mode, approaching a satellite for attack can take minutes to hours. Widespread build-up of ASAT weapons could lead to first-strike fears and incentives for pre-emption. Arguing that "[s]pace is the world's newest warfighting domain",[13] in 2018 the USA decided to build up a space force, the size and shape of which is not yet clear.

---

[10] Matt Korda, Hans M. Kristensen (2019), US ballistic missile defences, Bulletin of the Atomic Scientists 75 (6), 295-306, DOI: 10.1080/00963402.2019.1680055.

[11] Joseph N. Pelton (2019), Space Weapons, the Threat of War in Space and Planetary Defense, in Joseph N. Pelton, Space 2.0 – Revolutionary Advances in the Space Industry. Cham: Springer Nature; Bulletin of the Atomic Scientists (2019), Special Issue Space, 75 (4).

[12] Space weapons: based in space or acting against space objects,

[13] US DoD (Department of Defense) (2019), Trump Signs Law Establishing U.S. Space Force, by Jim Garamone,

The Outer Space Treaty only prohibits weapons of mass destruction in space; proposals for a general space-weapon ban were not taken up.

Hypersonic Missiles[14]

The term “hypersonic” is used for speeds above five times the sound speed (0.34 km/s = 1,200 km/h at normal temperatures). Hypersonic missiles come in two variants: hypersonic glide vehicles (HGVs) and hypersonic cruise missiles (HCMs).

In the USA projects date back to the 1960s. It developed and tested HGVs after 2003 for its “conventional prompt global strike” programme but ended it after tests in 2010 and 2011. Russia intensified work on hypersonic missiles in the 1980s, after the US SDI. It has developed both kinds and deployed them in 2018/2019. China is active in research and has tested HGVs from 2014 on. The USA has started new programmes for both kinds in 2016, giving them high priority.

A *hypersonic glide vehicle* (also called boost-glide vehicle) is thrown into space by a rocket. After this boost phase, it falls along an elliptical trajectory through outer space, similarly to a ballistic missile. But it reenters the atmosphere far in front of the target. At about 100 km altitude, it turns to horizontal and glides through the high atmosphere, descending to about 30 km while the speed decreases from about 6 km/s to about 2 km/s (20 to 6 times the sound speed). In this phase, covering many thousands of kilometres, the course can be changed by control flaps. Finally, the target is approached in a steep, guided descent. Alternatively, the vehicle stays below 100 – 200 km altitude all the time. The total range can exceed the maximum range of ballistic missiles (10,000 – 13,000 km). Depending on range, the flight time can be between 10 and 60 minutes.

Defence against HGVs is much more difficult than against ballistic missiles; the phase in space is shorter and at lower altitude so that the vehicles stay below the horizon of ground-based radars in the target region for longer. Space-based early warning systems can detect the rocket-launch flame and thus the launch and general direction. The trajectory part in space, if measured, would only allow a prediction of the reentry site. In the gliding phase an HGV can fly curves and, for example, circumvent BMD sites. This reduces the times for detection and for reaction considerably.

A *hypersonic cruise missiles* (HCM), on the other hand, does not leave the atmosphere. Its scramjet engine takes in air which limits the altitude to 30 km and requires initial acceleration, e.g. by aircraft or booster rocket. The speed of 1.7 to 2.7 km/s (5 to 8 times the sound speed) is 6 to 10 times that of traditional, subsonic cruise missiles, and 2 to 5 times that of supersonic combat aircraft. A range of up to a few thousand kilometres is possible. The flight

---

DOD News, Dec. 20, https://www.defense.gov/Explore/News/Article/Article/2046035/trump-signs-law-establishing-us-space-force/(13 Febr. 2020).

[14] James M. Acton (2013), Silver Bullet? Asking the Right Questions About Conventional Prompt Global Strike, Washington, D.C.: Carnegie Endowment for International Peace, http://carnegieendowment.org/files/cpgs.pdf (30 June 2020); James M. Acton (2015), Hypersonic Boost-Glide Weapons, Science & Global Security 23 (3), 191-219; Ajey Lele (2019), Hypersonic Weapons, in Ajey Lele, Disruptive Technologies for the Militaries and Security, Singapore: Springer Nature.

time for 1,500 km is 9 to 15 minutes, resulting in markedly shorter times for detection and reaction than the 80 minutes of subsonic cruise missiles.

HGV as well as HCM can carry conventional or nuclear warheads. All variants increase possibilities for surprise attack, in particular against strategic nuclear weapons and their command-and-control systems. Nuclear versions fall under New START, but whether this will be extended in 2021 is open; special rules for HGV and HCM would have to be added.

Autonomous Weapon Systems[15]

After significant proliferation of armed uninhabited air vehicles (UAVs), attacks by which are controlled remotely by human operators, the next step is being envisaged in military planning, research and development. Autonomous weapon systems (AWS) would—after activation—select and engage targets without further interaction with a human. The control program would analyse the sensor data, search for potential targets, classify them and attack the ones selected. There are precursors in defensive systems with an automatic mode and longer-range missiles with target recognition, but AWS for operating for a longer time in complex environments do not yet exist. AWS could move in the air, on or under water and on the ground.

AWS promise many military advantages. Operators are remote and less endangered. No radio link is needed that could be detected or jammed. Without involvement of a human and no need for communication over a distance, AWS could react much faster. However, there would be less control of events on the battlefield, and the systems could be hacked.

Introduction of AWS would lead to a much faster arms race than the one taking place at present with remote-control armed UAVs. This is because AWS are seen as important for combat against a competent adversary, not for very asymmetric scenarios. In the face of an AWS threat, one has a strong incentive to deploy AWS oneself.

Whether an algorithm can comply with international humanitarian law is doubtful. Another problem is the escalation dynamic from the interaction between two fleets of AWS at short mutual distance. With missile flight times of seconds, a very fast reaction would have to be programmed if the beginning of an attack is observed, otherwise one's systems could be destroyed before they could launch their missiles. In case of a false alarm, a "flash war" could start by mutual feedback.

Surprise attacks would be easier with AWS, raising nervousness and the pressure for faster reaction. A particular problem is posed by swarms that could attack from many sides, saturating defences. Swarm and swarm defence would become part of an AWS arms race.

---

[15] Nehal Bhuta, Susanne Beck, Robin Geiß, Hin-Yan Liu and Claus Kreß (eds.) (2016), Autonomous Weapon Systems – Law, Ethics, Policy, Cambridge: Cambridge University Press; Jürgen Altmann, Frank Sauer (2017), Autonomous Weapon Systems and Strategic Stability, Survival 59 (5), 117-142; Paul Scharre (2018), Army of None, New York/London: Norton.

AWS have been the subject of expert discussions in the context of the UN Convention on Certain Conventional Weapons since 2014, but due to opposition by militarily important states, limitations or a prohibition seem unrealistic in this framework. A prohibition of AWS will probably have to be sought outside of the CCW, similar to land mines and cluster munitions. Verification may have to work with after-the-fact investigations.[16]

Cyber-War Preparations[17]

Information and communication technology (ICT) has become central for military operations. This and the rise of the internet have motivated states to set up cyber forces, for defence as well as offence. War plans integrate physical attacks on enemy forces with attacks on their information systems. But attacks can also be limited to cyberspace, staying below the threshold of what would count as armed attacks that would justify self-defence in the physical world. Cyber attacks cover a wide spectrum, from intrusion into the military or civilian computer systems of an adversary to collect information, to destruction of the military or civilian infrastructure, severely affecting military operations or civilian life, comparable to the effects of massive physical attacks. In the latter case, plans for self-defence include responding with physical weapons, and international-law manuals are devising rules for war in cyberspace and the physical world.

Preparations for cyber war increase mutual threats, fear and mistrust, aggravated by secrecy. If malware had been planted in advance, cyber attacks could occur in seconds. This creates incentives to respond fast, by automatic reaction, possibly including artificial intelligence. Cyberspace is another area where fast escalation by interaction between two automatic/autonomous systems of attack and counter-attack has to be feared.

Arms control of cyber weapons and forces is difficult. Attacks can be launched by a multitude of actors, and the originator can be obscured. Cyber weapons—pieces of software—can be multiplied easily, defying numerical limits. Secrecy is easier than with missiles and aircraft. Concepts for limits on cyber forces and verification of compliance need intensive research.[18] As a first step, the confidence-building measures recommended by the UN and the OSCE should be expanded to cover cyber forces.[19]

---

[16] Mark Gubrud, Jürgen Altmann (2013), Compliance Measures for an Autonomous Weapons Convention, ICRAC Working Paper #2, International Committee for Robot Arms Control, 2013, https://www.icrac.net/wp-content/uploads/2018/04/Gubrud-Altmann_Compliance-Measures-AWC_ICRAC-WP2.pdf (30 June 2020).

[17] James A. Lewis, Götz Neuneck (2013), The Cyber Index – International Security Trends and Realities, Geneva: UN Institute for Disarmament Research, http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (11 Febr. 2020); Michael N. Schmitt (ed.) (2017), Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, Cambridge: Cambridge University Press; Christian Reuter (ed.) (2019), Information Technology for Peace and Security – IT Applications and Infrastructures in Conflicts, Crises, War and Peace. Wiesbaden: Springer Vieweg: chs. 4-7, 9-10, 12-13.

[18] For first ideas see Thomas Reinhold, Christian Reuter, Arms Control and its Applicability to Cyberspace, in Reuter (2019, op. cit.).

[19] Jürgen Altmann, Confidence and Security Building Measures for Cyber Forces, in Reuter (2019, op. cit.).

Nanotechnology[20]

Nanotechnology is an overarching term for many different areas, including electronics, materials and biological systems, the only common property being the scale of systems or components, namely with sizes between 1 and 100 nanometres (10^{-9} and 10^{-7} m). Among the particularly problematic military applications are small weapon systems, autonomous robots and new chemical/biological weapons. Regulation will have to be specific in each field.

Artificial Intelligence[21]

Artificial intelligence (AI) has advanced strongly in recent years and has become a field of major investment by companies and states. Big-data analysis and machine learning have brought impressive successes in games, in image recognition and in language translation. However, recognition can fail even if only minor changes are applied to an image. To make AI more compatible with human thinking, research is being done for explainable AI.

Major powers, foremost the USA, Russia and China, put great hopes in AI for their armed forces. AI is to take in more information, process it faster, leading to better decisions and allowing speedier action. Future AI may be transformative "on a par with nuclear weapons, aircraft, computers, and biotech".[22] AI could improve logistics, could control AWS and swarms thereof. In peace and in war, AI could find patterns in data from many sensors and other sources, improving situation awareness on all levels of military and military-political decision making. Actions of the enemy could be analysed and simulated. In the future, AI could move from decision support to decision making.

Machine learning for military operations suffers from a fundamental problem: there will not be many actual combat experiences from which to train the algorithms, different from games where there are fixed rules in a restricted space and millions of rounds can be generated by computer. Thus algorithm development and learning will have to rely heavily on simulated battles – but how certain can planners be that actual conflict would evolve

---

[20] Jürgen Altmann (2006), Military Nanotechnology: Potential Applications and Preventive Arms Control. Abingdon/New York: Routledge; Jürgen Altmann (2017), Preventing Hostile and Malevolent Use of Nanotechnology – Military Nanotechnology After 15 Years of the US National Nanotechnology Initiative, in Maurizio Martellini, Andrea Malizia (eds.), Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges: Threats and Counter Efforts, Cham: Springer International.

[21] Edward Geist, Andrew J. Lohn (2018), How Might Artificial Intelligence Affect the Risk of Nuclear War? Santa Monica CA: RAND, https://www.rand.org/pubs/perspectives/PE296.html(11 Febr. 2020); Michael C. Horowitz (2018), Artificial Intelligence, International Competition, and the Balance of Power, Texas National Security Review 1 (3), 37-57; Vincent Boulanin (2019), The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Volume I Euro-Atlantic Perspectives, Solna: SIPRI, https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk (11 Febr. 2020); Stanley Center for Peace and Development/United Nations Office for Disarmament Affairs/Stimson Center (2019/2020), The Militarization of Artificial Intelligence, https://www.un.org/disarmament/the-militarization-of-artificial-intelligence/ (29 July 2020).

[22] Greg Allen, Taniel Chan (2017), Artificial Intelligence and National Security, Cambridge MA: Belfer Center, Harvard University, https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf (16 Febr. 2020).

similarly? A stronger role of AI increases risks of hacking and deception. Human control would suffer, mainly by a much-increased speed of decisions and actions.

Concerning nuclear weapons, AI could play a role in early warning, attack characterisation and preparation of a counterattack. Principally even the launch decision could be delegated to AI. With more information processed, human decisions could be more appropriate, reducing the risk of accidental nuclear war, but the opposite is also possible. If big-data analysis could locate nuclear submarines or mobile intercontinental ballistic missiles, first-strike or crisis instability would ensue, in turn leading to arms-race instability.

Attempts to limit military AI uses meet many difficulties insofar as many applications would reside in internal ICT systems. AI in AWS could be prevented by an AWS ban. To prevent crisis instability, improved communication could help, but this would have to be at machine speed.

Additive Manufacturing[23]

Additive manufacturing (AM) or 3-D printing builds up parts layer by layer from liquid or powder material that solidify by various mechanisms, e.g. cooling from a melt or evaporation of a solvent. Plastic, metals and ceramics can be processed, and the strength of products approaches that from traditional technologies. The process is not well suited to mass production, but is useful for low numbers of special components and prototypes or for casting or pressing moulds. The machine and the available raw material set general conditions, but the shape of the product is nearly arbitrary, defined by the build file that consists of data that can be transmitted easily. With access to the build file, prohibited or limited products can be made. Crude firearms have already been produced, work is being done on ammunition and smaller missiles.

For armed forces, production of replacement parts in the field would reduce logistics. International security would be endangered if small uninhabited weapon systems could be mass-produced cheaply. Missile bodies as well as other components could be made. Additively manufactured parts could be used in centrifuges for uranium enrichment or for biological weapons.

Limiting military uses of AM seems difficult, some slowing down of proliferation may be possible by export control, but this would not affect the high-technology countries. If

[23] Trevor Johnston, Troy D. Smith, J. Luke Irwin (2018), Additive Manufacturing in 2040 – Powerful Enabler, Disruptive Threat, Santa Monica CA: RAND, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE283/RAND_PE283.pdf (11 Febr. 2020); Kolja Brockmann, Robert Kelley (2018), The Challenge of Emerging Technologies to Non-Proliferation Efforts – Controlling Additive Manufacturing and Intangible Transfers of Technology, Solna: SIPRI, https://www.sipri.org/sites/default/files/2018-04/sipri1804_3d_printing_brockmann.pdf (18 Febr. 2020); Grant Christopher (2019), Additive Manufacturing and the Military: Applications and Implications, in Christian Reuter, Jürgen Altmann, Malte Göttsche, Mirko Himmel (eds.), SCIENCE PEACE SECURITY '19 – Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research, Darmstadt: TUprints. https://tuprints.ulb.tu-darmstadt.de/id/eprint/9164 (11 Febr. 2020).

specific applications turn out as particularly problematic, it is rather these that should be made subject to arms control if they are not already (such as biological weapons).

Synthetic Biology, Gene Editing[24]

Since its start in the 1970s, genetic engineering has made enormous advances with DNA sequencing, modification and then synthesis. Synthetic biology produces artificial biological systems for fulfilling certain tasks and works for living systems that use different mechanisms. Several methods and tools have become widely accessible, coming within reach of hobby groups. There are concerns that individuals or groups could produce new harmful biological agents intentionally or by chance.

Since 2012, the CRISPR/Cas9[25] method has made genetic engineering drastically easier, allowing nearly arbitrary modification of DNA molecules ("gene editing"). Like other fundamental technologies, it has a dual-use capability. It promises healing of genetic diseases and has become an important tool of basic and applied research. Militarily it could be used to create new biological-warfare agents which of course would violate the Biological Weapons Convention (BWC) to which nearly all countries are parties. However, the BWC provides little obstacle for non-state actors. So-called gene drives to change or even eradicate animal or plant populations in the wild could also be used for hostile purposes. As genetic editing will be used more widely, the possibilities for malign uses will expand, increasing mistrust about what is happening in military R&D. That the BWC still has no compliance and verification protocol will aggravate the problem.

Enhanced Soldiers, Body Manipulation[26]

Far-reaching goals of manipulating body and mind have led to concepts of soldier enhancement, and military research began years ago. Detailed discussions about conditions, consequences and ethical issues have begun, but international security and preventive arms control are not yet taken into view. Among the possibilities mentioned are exoskeletons, changes of the biochemistry and brain implants. Visions include genetically modified "supersoldiers" and fully fledged cyborgs. Body, mind and mood could be modified; changes could be reversible or irreversible, maybe switched on or off. Obviously, such enhancements pose fundamental questions about the human condition and would involve the societies at large. Thus, it is open whether they will be used at all or within which bounds. But the promise of increased combat power can create strong military incentives, and the fear of

---

[24] Mirko Himmel (2019), Emerging Dual-Use Technologies in the Life Sciences: Challenges and Policy Recommendations on Export Control, EU Non-Proliferation and Disarmament Papers 64, EU Non-Proliferation and Disarmament Consortium, https://www.nonproliferation.eu/emerging-dual-use-technologies-in-the-life-sciences/ (11 Febr. 2020); Johannes L. Frieß, Anna Rössing, Gunnar Jeremias, Bernd Giese (2020). Application Scenarios for Gene Drives and new Biotechnology? Sicherheit + Frieden/Security and Peace, 38 (1), 29-35.

[25] Clustered Regularly Interspaced Repeats/CRISPR-associated protein 9.

[26] Alexander Kott, David Alberts, Amy Zalman, Paulo Shakarian, Fernando Maymi, Cliff Wang, Gang Qu (2015), Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report, ARL-SR-0327, Adelphi, MD: US Army Research Laboratory, https://www.arl.army.mil/arlreports/2015/ARL-SR-0327.pdf%20 (11 Febr. 2020); Marcus Wigan (2017), Ethics and Brain Implants in the Military, IEEE Technology and Society Magazine 36 (1), 65-68; Michael D. Matthews, David M. Schnyer (eds.) (2019), Human Performance Optimization: The Science and Ethics of Enhancing Human Capabilities, Oxford: Oxford University Press.

adversaries proceeding faster will weaken restraint. How international security would be affected would depend on the how widely and how intensely enhancement would be applied. Soldier enhancement would be accompanied by combat robots and AI, so it is probable that combat would move faster and decision times would be shorter.

5. Problematic Common Properties

Today one can foresee that the coming new technologies, if used by armed forces without constraints, would cause the international situation to deteriorate. They have properties in common that tend to increase threats and make arms control more difficult.

Wider Availability, Easier Access, Smaller Systems

Many generic technologies—information and communication technology, artificial intelligence, additive manufacturing and synthetic biology/gene editing—are becoming more widely accessible. Without big, state-funded laboratories, non-state actors, but also less capable states, could produce very dangerous items, in particular where products are defined by software with its relative ease of transfer. Dangerous objects could be very small, and production could take place in small facilities. Verification of limits on military uses would need the right to any-time, any-site inspections, and extensive monitoring of data traffic, that is, a degree of intrusiveness that armed forces as well as industry and civil society at large would have a hard time accepting.

Shorter Times for Attack, Warning and Decisions

In armed conflict as well as in a crisis, the time between detection of an attack and the (start of the) effect on the target is of utmost importance for a timely decision and possible reaction. This time is maximum if the launch can already be detected; it is smaller if the weapon can only be detected closer to the target. For physical carriers, the travel time is the upper limit; it depends on the speed and the distance covered. Table 1 lists the propagation times for various weapon types and typical distances. It shows that HCM drastically shorten the travel time compared to traditional cruise missiles. HGV need about the same time as ICBMs, but for the latter the target can be predicted from the trajectory through outer space, whereas the target of HGV can be found out only late in the second flight phase. The missiles from uninhabited weapon systems that are close to their targets would have flight times of seconds. If under remote control, reaction to an attack would be delayed by a few seconds due to the two-way communication; on the other hand, AWS could react immediately. Battle management using AI would accelerate the events. In case of cyber attacks, the network-propagation time varies between fractions of a second and a few seconds. If the target system(s) has been infected before, a cyber attack could occur within seconds. The effects may be noted with some delay, however.

The new military systems and technologies would reduce the time for decisions, and for double-checking whether indications of an attack are the result of a real one or of a malfunction or erroneous classification.

Table 1 Times from launch to arrival at target, or from start of attack to effects for various weapon types and typical distances. These times are upper limits for detection and warning of attack. Entries are typical or average values, for ballistic missiles for trajectories with minimum energy. The sound speed in air at 20 °C is 0.34 km/s, at -50 °C (10 km altitude) 0.30 km/s. For ballistic missiles and HGV, the speed at burnout is given; due to the elliptical flight path the speed decreases up to the peak altitude, and the path is longer than the distance along the ground. For anti-satellite weapons, the time varies between minutes and hours depending on the altitude and weapon type and deployment. HCM: Hypersonic Cruise Missile, ICBM: Intercontinental Ballistic Missile, HGV: Hypersonic Glide Vehicle, SLBM: Submarine-Launched Ballistic Missile. Source: Altmann (2020) (footnote 1).

Weapon Type	*Distance/ km*	*Speed/ km/s*	*Time to Arrival/ Effect*	*Nuclear*	*Conventional*
Subsonic long-range bomber	5,000	0.3	6 h	X	X
Supersonic fighter-bomber	1,500	0.5-0.9	50-30 min	X	X
Subsonic cruise missile	1,500	0.3	80 min	X	X
Supersonic missile	10	0.5-1.5	20-7 s	X	X
HCM	1,500	1.7-2.7	15-9 min	X	X
ICBM	10,000	7	33 min	X	-
HGV	5,000 + 7,000	6	24 + 24 min	X	X
SLBM	3,000	4.4	17 min	X	X
Cyber attack (prepared)	arbitrary	-	seconds	-	-

Conventional-Nuclear Entanglement

Faster, more precise missiles with conventional warheads, as well as AWS, could be used against strategic nuclear weapons and command-and-control systems. They could also be equipped with nuclear weapons. Smaller nuclear weapons are being deployed to deter conventional attacks. War among nuclear-weapon states would bring an increasing risk of escalation from conventional to nuclear weapons, and of regarding a conventional attack as nuclear-relevant. In a serious crisis, incentives for launch on warning and pre-emptive attack would rise.

6. Actual Situation and Fundamental Solution

In principle, the deterioration of international security from new technologies could be prevented or at least contained by corresponding prohibitions or limitations of military uses.[27] AWS could be banned, the BWC could be augmented by compliance and verification regulation. Space weapons could be prohibited, hypersonic missiles could be withdrawn again, and strong limits on ballistic missile defence could be re-introduced. Limits on cyber forces and verification of compliance pose conceptual difficulties and need creativity. Generic technologies can have many different military uses and will be wide-spread in civilian life. Limiting the most problematic developments could focus on the military applications and systems, but when they consist of software, very difficult problems of definition and verification arise; because of dual use, certain civilian applications would have to be included.[28]

Even though such limitations are urgent, the outlook for their implementation are dim in the present political situation. Arms control agreements are being dismantled. The nuclear situation is no longer a simple bipolar one; China is seen as becoming a relevant third player.[29] The UK and France, India and Pakistan, Israel and North Korea count at clearly lower levels.

Many countries strengthen their armed forces, with new technologies in the centre. A main driver (if not the main driver) of the qualitative arms race is the USA. The reason is its quest for military-technological superiority as a means to achieve military superiority, with the goal of providing "a decisive military superiority to defeat any adversary on any battlefield".[30,31] In 2015, the US DoD announced its "Third Offset Strategy". While the arguments for the first and second offset strategies had been a Soviet conventional superiority in Europe, the third one argues that Russia and China are catching up in military technologies and that the US needs fast advance "to sustain and advance America's military dominance

---

[27] Export control is insufficient – it can limit and delay proliferation to some countries and non-state actors, but cannot solve the problem of destabilisation among producer states.

[28] For examples how this could be done for applications of nanotechnology see Altmann (2006): ch. 7 (op.cit.).

[29] But it has to be noted that it is the USA and Russia that predominate in nuclear weapons, with 5800 and 6375 total warheads, respectively. China (320) is at a much lower level. SIPRI Yearbook 2020, Armaments, Disarmament and International Security, Summary, https://www.sipri.org/sites/default/files/2020-06/yb20_summary_en_v2.pdf (29 June 2020).

[30] "Superior technology has been, and continues to be, a cornerstone of the U.S. military's strategic posture. This was true during the Cold War, when technology provided superior conventional weapons for U.S. and allied forces. The same is true in today's Information Age which involves significant activity in the cyber domain. DOD Research and Engineering (R&E) programs are needed need to create, demonstrate, and partner in the transition to operational use of affordable technologies that can provide a decisive military superiority to defeat any adversary on any battlefield. Just as the past superior technologies have enabled an operational advantage for U.S. forces, continued technology development should enable future military superiority." US Department of Defense (2012), Defense Manufacturing Management Guide for Program Managers, October 16: Section 8.3, https://www.dau.edu/guidebooks/Shared%20Documents/Defense%20Manufacturing%20Management%20Guide%20for%20PMs.pdf (29 June 2020).

[31] The quest for US superiority is accepted as sensible and necessary by many academics in the USA, see e.g. the contributions in Margaret Kosal (ed.) (2020), Development, Use, and Proliferation of Disruptive and Game-Changing Technologies in Modern Warfare, Cham: Springer. Only rarely it is being put into question, e.g. Box 1.1 "Possible Ethical, Legal, and Societal Implications of Seeking Technological Superiority" (p. 40/41) in Jean-Lou Chameau, William F. Ballhaus, Herbert S. Lin (eds.) (2014), Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues, Washington DC: National Academies Press, http://www.nap.edu/catalog.php?record_id=18512 (30 June 2020).

for the 21st century".[32,33] Following the US role model, Russia and in particular China put much emphasis on AI for warfare, but in China there are also warnings of an arms race and risks to international security.[34]

By following military logic—and influencing many other countries—the three major powers, with the USA in the lead, are co-constructing a global future in which war-or-peace decisions will have to be taken not in minutes, but rather in seconds. More options of surprise attacks will increase fears and nervousness, favouring worst-case assumptions. The risk of misperceptions and false alarms will rise, by humans as well as by algorithms. This development could be stopped by preventive arms control, starting among the three, but then including other relevant countries.

All three powers should understand that their security cannot be guaranteed sustainably by ever-increasing, ever-accelerated military threats. The USA may be able to maintain technological superiority in some areas, but after a few years the others will catch up. In the face of China's growing economic power, it is questionable whether the US strategy can work in the long run anyway. Even if it could, continuous military-technological innovation will come at the price of much decreased stability and security for all, including the USA. If the USA will turn away from its superiority strategy, one can reasonably hope that Russia and China can be included in the process.

7. Conclusion: Back to Basic Insights

Stopping the slippage into an unstable situation needs a fundamental change. The leading powers need to accept the insight that sustainable national security is possible only in the context of international security, reducing military threats instead of increasing them. That the USA and the USSR in the past had partially accepted this is evident in the bilateral arms-control agreements. Particularly relevant is the statement from the Reagan-Gorbachev Geneva summit of 1985: "[A] nuclear war cannot be won and must never be fought."[35] Because conventional war between major powers carries a strong risk of escalation to

---

[32] Robert Work (2015), Deputy Secretary of Defense Speech, CNAS Defense Forum, Dec. 14, 2015, https://www.defense.gov/News/Speeches/Speech-View/Article/634214/cnas-defense-forum (30 June 2020).

[33] The Trump administration no longer mentions the offset strategy explicitly, but continues emphasising the need to maintain "decisive and sustained U.S. military advantages" or "overmatch" (US Department of Defense, Summary of the 2018 National Defense Strategy of the United States of America – Sharpening the American Military's Competitive Edge, 2018, p. 4, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf(30 June 2020); President of the USA, National Security Strategy of the United States of America, December 2017, p. 28, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf(30 June 2020)).

[34] Samuel Bendett (2018), Here's How the Russian Military Is Organizing to Develop AI, Defense One, July 20, https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/ (30 June 2020); Gregory C. Allen (2019), Understanding China's AI Strategy – Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security, Center for a New American Security, Febr. 6, https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy(30 June 2020).

[35] "The sides, having discussed key security issues, and conscious of the special responsibility of the USSR and the U.S. for maintaining peace, have agreed that a nuclear war cannot be won and must never be fought. Recognizing that any conflict between the USSR and the U.S. could have catastrophic consequences, they emphasized the importance of preventing any war between them. whether nuclear or conventional. They will not seek to achieve military superiority." Text of U.S.-Soviet Joint Statement. Issued in Geneva on November 21. 1985. UN General Assembly, A/40/1070, 17 December 1985, https://undocs.org/en/A/40/1070(29 June 2020).

nuclear, destabilising developments need to be prevented in nuclear as well as conventional forces.

In BMD, space weapons and hypersonic missiles, traditional mechanisms of arms control and verification can work. AWS and cyber operations need innovative approaches. The same holds for the generic technologies, where in particular the dual-use problem will have to be tackled. War prevention, reduction of threats and above all stability should be the overarching goals, with lengthening of warning and decision times a central means.

Preventing the rush to destabilising technologies requires nothing less than a fundamental re-orientation of the political and military strategies of the main actors. This is asking very much and at first sight may seem naïve and utopian, but it seems that the new military technologies are so intertwined with each other and so relevant for the future of the respective armed forces that a less comprehensive solution cannot work.[36],[37]

[36] There is a possible exception in the slight chance for a special AWS ban because AWS are not yet introduced and pose fundamental problems in several areas. However, to be effective the most important countries would have to participate, requiring at least a partial re-orientation.

[37] I am in good company here:

"At a time when saving even the shrunken nuclear strategic arms control regime between the United States and Russia and its imperiled remnants seems bleak, calling for a compendious, intricate, multidimensional approach to nuclear arms control admittedly has an air of fantasy about it. Anything less, however, will almost surely fall short as this exceedingly complex and potentially dangerous new multipolar nuclear world gradually threatens to spin out of control." Robert Legvold, The Future of Nuclear Arms Control, in Viatcheslav Kantor (ed.), Topical Issues of Nuclear Non-proliferation, International Luxembourg Forum on Preventing Nuclear Catastrophe,2018, http://www.luxembourgforum.org/media/documents/paris_2018_eng4_preview.pdf(30 June 2020).

"[U]topianism, the construction of effective global institutions, is the only realistic option. Putin and Trump clothe their actions in the language of traditional realism (statism and sovereignty) and this can only lead to war. The only way to address the problems that we face today is through a new or reformed set of institutions at international or global and local levels designed to facilitate the deployment of a new techno-economic paradigm that is ICT based and green and global." Mary Kaldor, Cycles in World Politics, International Studies Review 20 (2), 214-222, 2018. DOI: 10.1093/isr/viy038Kaldor 2018.

The Author

Jürgen Altmann is a physicist and peace researcher at TU Dortmund University in Dortmund, Germany. After a PhD in physics (1980, Universität Hamburg) since 1985 he has studied scientific-technical problems of disarmament. One focus is experimental research of acoustic and seismic sensors for monitoring in the context of co-operative verification of disarmament and peace agreements and of safeguards. Prospective assessment of new military technologies and analysis of preventive-arms-control measures form a second focus. Major studies have dealt with "non-lethal" weapons, the interactions between civilian and military technologies in aviation, military uses of microsystems technology and of nanotechnology, and armed uninhabited vehicles. Dr. Altmann teaches about the relationship of natural science, armament and disarmament and has authored chapters in corresponding text books.

Toda Peace Institute

The **Toda Peace Institute** is an independent, nonpartisan institute committed to advancing a more just and peaceful world through policy-oriented peace research and practice. The Institute commissions evidence-based research, convenes multi-track and multi-disciplinary problem-solving workshops and seminars, and promotes dialogue across ethnic, cultural, religious and political divides. It catalyses practical, policy-oriented conversations between theoretical experts, practitioners, policymakers and civil society leaders in order to discern innovative and creative solutions to the major problems confronting the world in the twenty-first century (see www.toda.org for more information).

Contact Us
Toda Peace Institute
Samon Eleven Bldg. 5th Floor
3-1 Samon-cho, Shinjuku-ku, Tokyo 160-0017, Japan
Email: contact@toda.org