ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

TECH-MILITARY REVOLUTIONS & THEIR SHIFTING IMPACT ON GLOBAL SECURITY

By
Abu Hurrairah
Intern
Arms Control & Disarmament Centre, ISSI

Supervised by
Ghazala Yasmin Jalil

October 3, 2022

(Views expressed in the brief are those of the author, and do not represent those of ISSI)

Tech-Military Revolutions

Over the years, new types of weapons that frequently gave a military edge have been made feasible by developments in science and technology. Most of the time, advancements in military technology happen gradually, but occasionally there are qualitative shifts that are so significant that they qualify as revolutions. One was characterized by the invention of firearms, while the other was by nuclear weapons. For over 30 years, the emergence of electronics, sensors, precise weapons, networked communication and a "system of systems" has been referred to as a "revolution in military affairs."

We are already in the midst of a more fundamental transformation. It will be characterized by cyber warfare, widespread military Artificial Intelligence (AI) uses, new genetics-related technologies, human body and mind manipulation and more widespread access to destructible technology.[1] Some most recent advancements are highlighted below.

Cyber-Technologies

The usage of information and communication technology (ICT) in military operations has become essential. States have created cyber armies as a result of the growth of the internet, both for

[1] Jürgen Altmann, "New Military Technologies: Dangers for International Security and Peace," *Sicherheit & Frieden* 38, 1 (2020).

offensive and defensive purposes. Attacks on the enemy's information systems are combined with physical attacks on their forces. Attacks can, however, be restricted to the virtual world and remain below the level of armed assaults that would call for self-defense in the real world. Cyber-attacks can damage military operations or everyday life just as severely as large-scale physical attacks. They can range from breaking into an adversary's military or civilian computer systems to gather intelligence to destroying their military or civilian infrastructure.

It is challenging to control the use of cyber weapons and troops. Numerous actors may initiate an attack, and the perpetrator may be hidden. Software-based cyber weapons can be easily multiplied, defying numerical restrictions. Compared to using missiles and aircraft, secrecy is simpler. In-depth research is required for the concepts of cyber force limitations and compliance verification.[2] The UN and OSCE advise that the confidence-building measures be extended to include cyber forces as a first step. [3]

Artificial Intelligence

Recent years have seen significant progress in artificial intelligence (AI), attracting considerable investment from businesses and governments. Game development, image identification and language translation have all benefited greatly from extensive data analysis and machine learning. Nevertheless, even with very slight image modifications, recognition can still fail. Research on explainable AI is being done to make it more logically consistent with human thought.

The US and Russia are two major powers with high expectations for AI in their military forces. With the ability to analyze information more quickly and with more volume, AI will enable quicker decision-making and action. AI's potential future impact is "on a par with nuclear weapons, aircraft, computers and biotech."[4] AI may aid in early warning, characterizing an attack and planning a counterattack in relation to nuclear weapons. In future, launch decisions may perhaps be handled by AI.

Nano-Techs

Electronics, materials and biological systems are all included in the broad category of "nanotechnology," The sole shared characteristic is the scale of the components, which is defined as

[2] Thomas Reinhold and Christian Reuter, "Arms Control and its Applicability to Cyberspace" in Christian Reuter (ed) *Information Technology for Peace and Security*, (Wiesbaden: Springer Vieweg, 2019)

[3] Ibid.

[4] Allen Greg and Taniel Chan, "Artificial Intelligence and National Security." Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2017, https://www.belfercenter.org/publication/artificial-intelligence-and-national-security

being between 1 and 100 nanometers (10-9 and 10-7 m).[5] Small weapon systems, autonomous robotics and new chemical and biological weapons are a few of the military uses that pose specific problems. Each field's regulation will need to be precise. [6]

Gene Modification

Genetic engineering has come a long way with DNA sequencing, modification and synthesis since it first emerged in the 1970s. Synthetic biology develops artificial biological systems to carry out certain functions and functions for living systems that employ various methods. Numerous techniques and equipment have improved accessibility, making them available to hobby groups. It's possible for people or organizations to intentionally or accidentally create new hazardous biological agents.

Since 2012, genetic engineering has become significantly simpler because of the CRISPR/Cas9[7] technique, which permits practically arbitrary change of DNA molecules (also known as "gene editing"). It has a dual-use capability, just like other vital technologies. It promises to cure genetic illnesses and has developed into a crucial tool for fundamental and applied research. It might be used militarily to develop new biological warfare weapons, which would be against the Biological Weapons Convention (BWC), to which almost every state is a party. The BWC, however, does not present many challenges for non-state actors. It is possible to deploy so-called gene drives with malicious intent to alter or even wipe out wild populations of animals or plants. The potential for malicious applications of genetic editing will grow as its use spreads, raising concerns about what is being done in military R&D. The fact that the BWC currently lacks a compliance and verification methodology can worsen the issue.

Super Soldiers

Military research started years ago with the long-term goal of modifying the body and mind to create conceptions of soldier augmentation.[8] The conditions, repercussions and moral dilemmas are

[5] Jürgen Altmann, "Preventing Hostile and Malevolent Use of Nanotechnology Military Nanotechnology After 15 Years of the US National Nanotechnology Initiative," *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges: Threats and Counter Efforts*, eds. Maurizio Martellini and Andrea Malizia (Cham: Springer International Publishing, November 2017), https://link.springer.com/chapter/10.1007/978-3-319-62108-1_4#chapter-info.

[6] Jürgen Altmann, *Military Nanotechnology: Potential Applications and Preventive Arms Control* (Routledge, December 2005), https://doi.org/10.4324/9780203963791.

[7] Maria G Detsika et al., "Generation of a Novel Decay Accelerating Factor (DAF) Knock-out Rat Model Using Clustered Regularly-Interspaced Short Palindromic Repeats, (CRISPR)/Associated Protein 9 (Cas9), Genome Editing," *Transgenic Research* 30, 1 (January 2021), https://rdcu.be/cVXFm.

[8] M Wigan, "Ethics and Brain Implants in the Military [Commentary]," *IEEE Technology and Society Magazine* 36, 1 (March 2017), Doi: 10.1109/MTS.2017.2654292.

being discussed in great detail, but international security and preemptive arms control are not yet in the picture. Exoskeletons, modifications to biochemistry and brain implants are a few of the hypothetical options proposed. Some people have visions of fully developed cyborgs and genetically enhanced "super soldiers." Changes can be made to the body, mind and mood; they might be reversible or irreversible, switched on or off, etc.

Of course, such improvements raise important issues for society and fundamental questions about the human condition. As a result, it is uncertain whether or how they will be used.[9] Though the threat of faster-moving enemies will make restraint less effective, the promise of greater battle power might generate powerful military incentives. The extent and degree to which improvements are implemented will determine how they impact international security. Combat would likely go faster, and decisions would be made quicker since soldier upgrading would be combined with combat robots and AI.[10]

Possible Challenges

Today, it is possible to predict that if armed forces employed upcoming new technology unrestrainedly, the global situation would get worse. They share traits that often lead to greater threats and more difficulty enforcing arms control.

Information and communication technology, additive manufacturing, artificial intelligence and synthetic biology/gene editing are just a few general technologies that are becoming more broadly available. Without large government laboratories, less skilled states and non-state players alike could develop hazardous goods, particularly in industries where products are defined by software due to its comparatively simple transmission. Small production facilities and dangerous items of all sizes are also possibilities. Armed forces and the general public would find it difficult to accept the intrusiveness required to verify the limits on military uses, including the right to anytime, anywhere inspections and effective data traffic monitoring.

Recommendations

It is possible to stop the degradation of global security brought on by new technology by prohibiting or restricting military applications. A few recommendations in this regard are:

[9] M D Matthews and D M Schnyer, *Human Performance Optimization: The Science and Ethics of Enhancing Human Capabilities* (Oxford University Press, 2019).

[10] Alexander Kott et al., "Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report," Army Research Lab Adelphi Md Computational and Information Sciences Directorate, June 2015, https://apps.dtic.mil/sti/citations/ADA621223.

- There should be proper and systematic regulations and verification mechanisms in BWC.
- Limits should be there for cyber forces, and more creative ideas should be discussed for better civilian use.
- Generic technology should be widely used for the betterment of civilian lives rather than focusing on military applications solely.
- Military applications and systems may be targeted as the most problematic advancements to limit, but when they are software-based, highly challenging definition and verification challenges arise; due to their dual use. Thus, specific civilian applications should need to be included in this paradigm.[11]

Many states upgrade their military forces, putting modern technologies at the forefront. The US is a significant force behind the qualitative arms race. There are several reasons for this, including the US's pursuit of military-technological superiority to achieve military supremacy to provide "a decisive military superiority to defeat any adversary on any battlefield."[12] If the US abandons this strategy, it is reasonable to expect that other nations will be able to participate in the process as well.

Conclusion

A major adjustment is required to stop the deterioration into an unstable state. The superpowers must acknowledge that long-term national security is feasible only within the global security framework and that this requires diminishing rather than escalating military threats. Adaptive strategies are needed for cyber operations. Similar circumstances apply to generic technology, where it will be necessary to address the dual-use issue. The main objectives should be to avert war, lessen threats and, most importantly, maintain stability, with a key strategy being to extend warning and decision times. Although it may initially appear utopian, the new military technologies are so linked and crucial to the future of the respective armed services that a less comprehensive solution is unworkable. [13]

[11] Ibid.

[12] National Research Council, "Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues: Summary," 2014, https://doi.org/10.17226/18512.

[13] Robert Legvold, "The Future of Nuclear Arms Control: Topical Issues of Nuclear Non-proliferation," International Luxembourg Forum on Preventing Nuclear Catastrophe, 2018, https://www.luxembourgforum.org/media/documents/paris_2018_eng4_preview.pdf.