Defence Research and Development Canada | Recherche et développement pour la défense Canada

CAN UNCLASSIFIED

DRDC | RDDC
technologysciencetechnologie

Biotechnology, Human Enhancement and Human Augmentation: A Way Ahead for Research and Policy

Dr. Gitanjali Adlakha-Hutcheon
DRDC – Centre for Security Science

Dr. Matthew T. Richins
Defence Science and Technology Laboratory, DSTL

Dr. Deborah E. Taylor
Air Force Research Laboratory

NATO Science and Technology Organization (STO)

STO Technical Report
TR-HFM-ST-335-A

Date of Publication from Ext Publisher: December 2021

Defence Research and Development Canada

External Literature (N)
DRDC-RDDC-2022-N108
March 2022

Canada

2.0 RECOMMENDATIONS FOR A WAY AHEAD

The emergence of novel enhancement technologies brings with it numerous, significant implications, which challenge the ethical, moral, and legal dimensions of modern democratic society. For Defence, the issues are both symbolic and realistic; threatening to erode the human values of character and virtue in service but also potentially risking the safety of personnel or limiting the scope of their role, given new, unique vulnerabilities to security and data integrity.

2.1 Security and Compliance Considerations

2.1.1 Societal Considerations

On a societal level, enhancement to Defence and Security personnel may be rejected by sections of society, particularly where radical augmentation is perceived. This may further exacerbate the distance of understanding from a civilian population to its serving military. Such resistance could influence the pace of technological development or national adoption. It will be the role of local government to facilitate ongoing discourse and engagement reaching across state and society.

2.1.2 Temporal and Permanence Considerations of Technology Adoption

Adoption of novel technologies will vary depending on the extent and permanence of change, and the inherent associated risks. Moderate enhancement (which are impermanent, temporary and non-invasive, for example: wearable technology or nutraceuticals) are likely to fit into existing domestic legal, ethical, and political frameworks. However, more invasive technologies, likely also permanent with potentially greater gains in efficacy but greater risks (e.g., implanted brain computer interfaces or genetic editing) will necessarily require new legal definitions for adoption or prohibition depending on the ruling of domestic and intentional bodies (see tables provided in the Military Medicine, Force Protection, and Warfighter Performance chapters in Naik et al, 2021 [5]). The implementation of new law or the amendment of existing law will require the efforts and involvement of scientists, lawyers, medics, and bioethics experts. In addition, more radical approaches to policy development may be required in order to keep pace with technology development and ahead of adversarial adoption (Triggered Recommendations 1 and 2).

2.1.3 Compliance Considerations

From a Compliance perspective, the autonomy of individual states may create an uneven landscape in terms of legal definitions. Where domestic law may vary, it will be the onus of international bodies (such as NATO and the United Nations) to provide an agreed legal framework for the use of biotechnologies for human enhancement. The absence of such effort will impact on interoperability between allies and maneuverability against the adversary (Triggered Recommendations 3 – 5).

The Security and Compliance team considered the enhancement and augmentation of human performance at the physical, sensory, and/or cognitive levels through technologies including devices or biotechnology (including at the genetic level therefore includes consideration of synthetic biology; again guided by tables from other pillars, in particular by Warfighter Performance (e.g., biosensors, implanted and wearable devices, exoskeletons, etc. see Naik et al, 2021 [5])) and promising areas for innovation in Military Medicine such as immunizations, medications for environmental threat prophylaxis, and therapeutics.

2.1.4 Security Considerations

From a Security perspective, there are security concerns arising from citizen biohacking. That is, members of the public who experiment on themselves, by implanting devices in their body (such as Radio Frequency

Identification (RFID) tags, Light Emitting Diodes (LEDs), temperature sensors, etc.) and share their experiences within relatively closed communities. This has implications to the fields of medicine, law enforcement, border control, customs, and the military, in addition to challenging the development and implementation of effective regulation. For the military, for example, bespoke implants which generate, transmit, and receive data could possibly prohibit interoperability, with allied forces, or with existing capabilities/systems. Efforts should be pursued to understand the implications of this kind of biometric data storage for the armed forces (Triggered Recommendation 6).

Defence (warfighters) and Security personnel are already using technologies that may inadvertently lead to safety/security issues (e.g., wearables/apps revealing secret military locations). A number of militaries are collating genetic information (genomic data) with medical data from their service personnel to find linkages between genes, military exposure, and health. Likewise other nations are exploring the use of such data to identify and enhance their warfighters. The predictive value of genomic data is currently limited, however as the technology advances there may be increasing threat from forging biomedical data, identifying individuals, and using biological information to infer the battlefield. It is recommended that an international effort is made to keep a watching brief on advances in this area as well as to understand the wider implications of new security vulnerabilities emerging from convergence of genomic and biometric data (Triggered Recommendation 7).

The issue is not only that technology is evolving faster than regulatory frameworks but the exacerbation with differences in ethical, moral, and legal perspectives across nations in regard to human enhancement and augmentation. In an effort to better address this, the current landscape of BHEA; and mitigate against the Security and Compliance (including legal and ethical) challenges now and into the future, the team has developed the following recommendations for consideration in terms of Compliance, followed by two within the realm of Security.

2.2 Recommendations for NATO-HFM

Compliance Related Recommendations for NATO-HFM

Listed below are compliance related recommendations for follow-on work/agenda setting options for NATO-HFM. HFM Research Specialist Team(s) should be established to:

2.2.1 Stand up an operational bioethics panel

Stand up an Operational Bioethics Panel, whose remit[6] would be to provide ongoing independent oversight and advice on research and the pursuit of implementation of biotechnologies for human enhancement by constituent nations. Such pursuit should include an NATO HFM activity to determine the scope and regularity of need of coming together of the Operational Bioethics Panel. The membership must be multidisciplinary, include at a minimum scientists, ethicists, medics, lawyers, and end-user operators.

2.2.2 Conduct trend analysis on EDT research, development and use

Conduct a trends analysis on developments that could lead to changes in behavior, strategy, or policy (i.e., 'weak signals'), for example from BHEA developments in lower levels of technical maturity and operational application. The impact of this activity would be aid in anticipatory / a priori policy initiation associated with BHEA within the EDT's rather than reactionary policy in response to an unforeseen incident.

[6] Refer to work of the US NIH NExTRAC (Novel and Exceptional Technology Advisory Committee; [6]) and adapt.