Digital Rights and Armed Forces Personnel – OSCE ODIHR Background Paper

Draft – 24/09/2021

Introduction

This background paper examines the impact of digital technologies on the human rights of armed forces personnel (AFP). The OSCE Code of Conduct on Politico-Military Aspects of Security (the Code of Conduct) states that "Each participating State will ensure that military, paramilitary and security forces personnel will be able to enjoy and exercise their human rights and fundamental freedoms as reflected in OSCE documents and International law, in conformity with relevant constitutional and legal provisions and with the requirements of service."[1] This background paper will therefore scope out the implications of new technological developments that may be used by or for AFP for their human rights and fundamental freedoms with reference to OSCE documents and international law.

The development of technology in the military sphere has significant implications for human rights more broadly and topics including the use of autonomous weapons and medical enhancements among others have been the subject of much ethical debate. The focus of this paper is on the ways digital technologies affect the human rights and fundamental freedoms of AFP themselves. While the focus is on international law relating to human rights and fundamental freedoms, in practice, these rights will also be reflected in national laws and constitutions, some of which may be more developed in certain areas than the current international standards. It includes an assessment of both negative and positive potential consequences of existing and developing technologies on AFP. Human rights laws are recognised as "living instruments" under international law, this means that human rights develop over time to respond to changing conditions. The rapid acceleration of various kinds of technological developments that may be used by or on AFP calls for new perspectives on the ways that AFP human rights and fundamental freedoms must be protected in the modern context.

There are a broad range of technological and scientific developments that may affect the rights and freedoms of AFPs such as biochemical enhancements and other medical interventions. This introductory background paper, however, will consider the implications of digital technology in particular. It is divided into two broad sections. The first on digital enhancement and digital warfare deals with the ways new and emerging technologies may affect the mental wellbeing, mental and physical integrity and related rights and freedoms of AFP. The second looks at the consequences of big

[1] At paragraph 32

data, digital footprints and the issue of accountability in the digital sphere for the human rights and freedoms of AFP. This background paper is designed to advance thinking around the practical consequences of new and developing digital technologies for AFP in the OSCE region and to build on the existing work in the Human Rights of Armed Forces Personnel: Compendium of Standards, Good Practices and Recommendations.

1. Digital Enhancement and Digital Warfare

- Brain-computer interfaces

"A brain–computer interface (BCI)[2] is a system that measures activity of the central nervous system (CNS) and converts it into artificial output that replaces, restores, enhances, supplements, or improves natural CNS output, and thereby changes the ongoing interactions between the CNS and its external or internal environment."[3] Effectively, BCI's are technologies that allow direct communication between the brain and a computer without the need for an input or output method such as speech, reading or typing to convey messages. BCI's already exist in some contexts. They can be used to restore lost functions such as speech or movement, they can support renewed control over the body, for example through the stimulation of muscles or nerves to allow control over a hand or other body part. They could also be used to enhance function, for example by prompting someone falling asleep at the wheel to wake up. Most BCIs developed to date use electrical signals that are detected through using electrodes either invasively within or on the cerebral cortex or non-invasively on the scalp. Some have also been based on metabolic activity measured non-invasively.

As well as BCIs developed in the medical context, in recent years, technology companies have looked into the potential for developing BCI's for a wider range of purposes. For example, Neuralink claims that it is "designing the first neural implant that will let you control a computer or mobile device anywhere you go. Micron-scale threads are inserted into areas of the brain that control movement. Each thread contains many electrodes and connects them to an implant, the Link."[4] It says "the Neuralink app would allow you to control your iOS device, keyboard and mouse directly with the activity of your brain, just by thinking about it."[5] In 2017, Facebook announced ambitious plans to develop a non-invasive head-mounted BCI, but in 2021 it announced that it had abandoned those

[2] Also sometimes called a Brain-machine Interface (BMI)

[3] Brain-Computer Interface - an overview | ScienceDirect Topics

[4] Approach - Neuralink

[5] Approach - Neuralink

plans in favour of developing wrist-based electromyography as the primary input for its Augmented Reality (AR) glasses.[6]

In the military context, researchers have "anticipated that BCI capabilities could enhance the speed of communication, improve common situational awareness, and allow operators to control multiple technological platforms simultaneously."[7] Other potential uses included monitoring the cognitive workload of AFP, controlling drone swarms and linking to prosthetics. The uses of BCIs in the military context can be divided into several types: data transfer from the brain, direct system control, prosthetics and paralysis treatment, cortically coupled AI (for training or running AI systems), data transfer to the brain, and brain-to-brain communication.

Human rights implications of BCIs

The different types and uses of BCIs raise different concerns and opportunities for the rights and freedoms of AFP. The following is a brief overview of potential implications for human rights according to type and use of different BCIs.

- BCIs in the medical context

The development of BCIs that can restore physical function can be viewed as a benefit for AFP injured in the context of their work. The potential to restore speech or physical function such as control of hands or limbs or the ability to control prosthetics can have a positive impact on the lives and well-being of AFP dealing with serious and life-changing injuries in the course of their service. This kind of development may restore dignity and improve mental health of affected AFP with implications for the right to life against the backdrop of suicide risk amongst veterans[8] as well as the rights to physical and mental integrity.

However, recent research has shown that suicide rates among US veterans in the post 9/11 era are four times higher than veteran suicide rates in the decades before that. One of the possible reasons the researchers gave for this phenomenon was the "sheer length of the war in tandem with advances in technology and medicine that see service members redeployed after severe injuries. A byproduct of the protracted war and the contemporary advancements in equipment, technology, and medicine is more service members survive and live to fight another day, tasked with returning to

[6] Facebook shows off how you'll use its neural wristbands with AR glasses - The Verge

[7] Brain-Computer Interfaces: U.S. Military Applications and Implications, An Initial Assessment | RAND

[8] Military Suicides for Post-9/11 Veterans Are High, Study Warns - The New York Times (nytimes.com) and Suitt_Suicides_Costs of War_June 21 2021.pdf (brown.edu)

combat after surviving." So, while medical uses of BCIs can have a positive therapeutic impact for AFP in terms of mental and physical wellbeing, where they are used to prepare injured AFP for redeployment, this may be damaging.

- BCIs for enhancement

The use of BCIs for either cognitive or physical enhancement to improve the effectiveness of AFP in warfare raises a different set of ethical and human rights questions. BCIs may be invasive using surgically inserted technology or non-invasive using external electrodes to read brain signals. Both types of BCIs, where they are being used to monitor the brain activity of AFP raise serious concerns of the mental integrity and mental privacy of AFP. The right to freedom of thought also provides absolute protection for the right to keep one's thoughts private. Technology that can access the brain activity of AFP directly could, in certain circumstances, interfere with that right.

In the case of non-invasive BCIs, AFP may be able to remove the technology that effectively monitors their brain activity, reducing the potential impact on mental privacy. But there may be questions around the possibility in practice for AFP to refuse the use of BCIs. Informed consent to the use of non-invasive BCIs that provide direct access to brain activity is a complex issue in the context of AFP. If BCIs become an increasingly common element of modern military activity, the potential for AFP to refuse to use BCIs may be limited.

In cases where AFP do consent to the use of non-invasive BCIs, consideration must be given to the way the information gathered through the BCI may be used to the detriment of AFP. If, for example, monitoring of brain activity revealed thoughts or mental states that resulted in disciplinary proceedings or negative outcomes for an individual, this could also be considered as a violation of the right not to be penalised for thoughts alone protected under the absolute right to freedom of thought.

Invasive BCIs for enhancement raise further concerns around the need for informed consent. Surgical procedures that are designed to enhance AFP capabilities for warfare involve both physical and moral risks. The process for inserting invasive technology may be dangerous and there could be risks of infection or adverse reactions to surgery. Surgery involving the brain could have life changing and even life threatening consequences where there are complications. The inability to remove invasive BCIs easily also poses risks for mental privacy, the right to freedom of thought and human dignity of AFP. There may be significant mental or physical consequences over the long term of invasive techniques.

BCIs that are designed to transfer data to the brain or for direct brain to brain communication also raise questions of autonomy and the risk of manipulation which could have negative impacts on AFP rights to freedom of thought. This may be particularly relevant where BCIs could be used to override individual decision making, instinct, autonomy and moral agency in relation to actions taken by AFP. Researchers have noted that there is already a dissonance between the ways that military culture and training limit individual AFP's agency and the individual moral responsibility laid on individuals when things go wrong.[9] The potential loss of agency over actions may contribute to the possibility of "moral injury" that is increasingly recognised by psychiatrists.[10] In the context of military service, "moral injury" refers to the "lasting emotional, psychological, social, behavioural, and spiritual impacts of actions that violate a service member's core moral values and behavioural expectations of self or others."[11]

- Psychosocial impact of remote or automated warfare – positives and negatives compared to traditional combat

Warfare is increasingly automated and remote. Drone strikes and autonomous weapons raise ethical and human rights concerns for the communities they are used on,[12] but from the perspective of this background paper, they may also pose human rights issues for AFP using them. While the physical risks of engaging remotely in warfare may be more limited than involvement in direct combat, there are increasing studies to indicate that drone operators, for example, may suffer psychological impacts comparable to those affecting the pilots of manned aircraft.[13] Remote warfare is, therefore not risk free. The potential psychological consequences including, for example PTSD, may have implications for AFP's rights to private and family life and related rights and may have a serious impact on their ability to form and maintain relationships. They could also have consequences for economic, social and cultural rights including the right to work where the

[9] Suitt_Suicides_Costs of War_June 21 2021.pdf (brown.edu) / Crawford, N. (2013). Accountability for Killing Moral Responsibility for Collateral Damage in America's Post9/11 Wars. New York, NY: Oxford University Press, p. 225

[10] https://moralinjuryproject.syr.edu/ Suitt_Suicides_Costs of War_June 21 2021.pdf (brown.edu)

[11] https://moralinjuryproject.syr.edu/

[12] Autonomous weapons systems, killer robots and human dignity | SpringerLink

[13] Robert Sparrow, "Drones, Courage, and Military Culture," in *Routledge Handbook of Military Ethics*, ed. George Lucas (Oxon: Routledge, 2015) Drones-courage-and-military-culture.pdf (robsparrow.com)

psychological impact is such that AFP can no longer continue to work in the military context or afterwards.

A recent Australian study of the attitudes of AFP to deployment in a MUM-T (manned unmanned teaming) showed that there was a quite high degree of reticence to be deployed in situations where the AFP had less control over the machines and ultimately over decision making in warfare.[14] The use of human-machine teams, may well raise serious moral questions for AFP which could engage the right to freedom of conscience. However, the same study highlighted the reduced risk of harm for AFP deploying autonomous weapons as a significant perceived benefit by AFP themselves.[15]

One of the challenges for future warfare is the over-abundance of data available through Internet of Things (IoT) connected devices, AFP worn sensors and other sources of information which can lead to cognitive overload. Researchers have noted that BCIs may be able to enhance the speed and accuracy of human decision making in a situation of information overload. DARPA gives the potential ability of military personnel to "facilitate multitasking at the speed of thought" and "interface with smart decision aids" as justifications for its investment in noninvasive or minutely invasive BCI technologies.[16] Technological developments in warfare more broadly may lead to AI enabled battlefields or what US scholars have referred to as "hyperwar"[17] in which the speed and scale of information to be processed on the battlefield would mean that BCIs may be the only way to maintain human decision-making in combat situations.[18] In these circumstances, BCIs may offer an opportunity for accountability and human moral judgement to retain a place in the increasingly autonomous modern battleground.

2. Digital Footprints and Accountability

While BCIs may feel more futuristic, there are many ways that digital technology already affects the rights of AFP in their daily lives and in the context of warfare. The digitilisation of so many aspects of life and the ubiquity of connected devices, in particular smartphones, means that concerns around

[14] Risks and Benefits of Autonomous Weapon Systems: Perceptions among Future Australian Defence Force Officers > Air University (AU) > Journal of Indo-Pacific Affairs Article Display

[15] Risks and Benefits of Autonomous Weapon Systems: Perceptions among Future Australian Defence Force Officers > Air University (AU) > Journal of Indo-Pacific Affairs Article Display

[16] Defense Advanced Research Projects Agency, "N3 Proposers Day," press release, April 3, 2018. (cited in Rand)

[17] Amir Husain, Hyperwar: Conflict and Competition in the AI Century, Austin, Tex.: SparkCognition, 2018. (cited in Rand)

[18] Rand, p.13-14

personal data and connectivity are significant for AFP. This includes their engagement with their families and communities through social media and electronic communications, but also the use of data in many other spheres including human resources and accountability mechanisms. Many of these discussions are relevant to human rights in general but there are some specificities of AFP which raise novel angles to concerns about privacy, freedom of expression and data protection.

- Social media and personal connected devices

The use of social media can support the right to freedom of expression and allow AFP to communicate with loved ones and their home communities even when they are far from home. But the security risks associated with social media use by AFP justify a degree of restriction on their use. As the US Department of Navy put it "Loose tweets sink fleets."[19] Social media posts, including photographs, can give huge amounts of information beyond the content of a particular post with metadata potentially revealing the location of deployment and other data that the poster may not be aware of. Similarly, connected fitness devices can leak crucial information about the location of AFP which could pose serious security concerns and put lives at risk.[20] Restrictions on social media use by serving AFP may well be a proportionate interference with the right to freedom of expression and related rights of AFP. Limitations on the use of social media and other methods to maintain connections with friends and family and to engage with community debates may have implications for other rights of AFP including the right to private and family life, the right to freedom of association and the right to freedom of opinion which includes access to information. The increasing problem of disinformation online also raises concerns about the right to freedom of opinion which includes the right to form opinions free from manipulation. Policies around the use of social media and other networked communications and personal connected devices by AFP should take a holistic view of human rights risks and benefits.

- Data protection, personnel files and automated decision making

The protection of personal data is particularly important in relation to the use of digital technologies for management of personnel and human resources. Cybersecurity is crucial to protecting the privacy of AFP in relation to data held on their personnel files to prevent unauthorised access which could put lives in danger. But there are significant risks associated with the collection and storage of personal data, in particular biometric data which identifies AFP based on immutable characteristics. The withdrawal of international troops from Afghanistan highlighted the danger of large biometric

[19] Security Awareness "Loose Tweets, Sink Fleets" (livingsecurity.com)

[20] Strava Fitness App Can Reveal Military Sites, Analysts Say - The New York Times (nytimes.com)

databases falling into the wrong hands. Biometric databases collated to address fraud in the Afghan security services were left exposed when the Afghan government was taken over by the Taliban.[21] Leaks of personal data in the context of AFP can have dire consequences for the lives and safety of AFP and their families. Data protection in this context is a right which may be a matter of life or death for AFP and potential future risks should be borne in mind as well as current contexts.

Technological developments in the field of personnel management and human resources increasingly use machine learning and artificial intelligence to assess candidates or personnel using automated decision-making. When technology is used in the interview or selection process, care needs to be taken to ensure that bias in the data does not taint the decision making process with discriminatory outcomes.[22] Similarly, using AI to detect fraud or other issues in AFP, may compound discrimination by ascribing suspicion to certain groups of AFP inferring dishonesty based on cultural, physical or other characteristics based on bias in the data. Large pools of data may also risk ascribing guilt by association where decisions are based on the personal data not only of an individual, but also of their family, social and professional connections. Where automated decision making processes are not transparent, they exacerbate the potential impact on the rights of AFP including the right to private and family life, the right not to be discriminated against and employment related rights.

- *Whistleblowing and digital complaints mechanisms*

Digital technologies provide new opportunities for whistleblowing and digital complaints mechanisms that may support AFP but may also expose them to additional risks. Digital internal complaints mechanisms can allow AFP to raise concerns about human rights violations, corruption or other issues without having to broach these issues with direct superiors. The ability to make complaints through an online or digital platform therefore improves accessibility of complaints mechanisms and may assist in highlighting and addressing systemic problems that undermine the rights of AFP in the workplace.

The possibility of accessing huge amounts of data in the digital environment, however, can create opportunities for whistleblowers to share extensive information as seen in the case of Chelsea Manning, who shared hundreds of thousands of classified and sensitive documents with Wikileaks resulting in her conviction and imprisonment. Effective channels for whistleblowing are an important

[21] This is the real story of the Afghan biometric databases abandoned to the Taliban | MIT Technology Review

[22] Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development | SpringerLink

aspect of accountability but the digital environment means that the amount of information that can be accessed and shared is potentially unmanageable and may create security threats for AFP as well as exposing AFP whistleblowers to legal risks.

- *Fair trial rights and new technologies*

Digital technology provides new opportunities for identifying verifiable evidence, but also carries the risk of the creation of deep fakes and other types of information that may obscure the truth. The use of digital technologies to create deep fakes can be fuel misinformation and may be used by hostile states as well as non-state actors. They may be fake representations of people, including AFP to provoke hatred or outrage, or they may be falsified information such as deep fake satellite images to mislead military strategists or cover over evidence of atrocities.[23] The implications for AFP could be direct, for example where a deep fake features images of them, or indirect, for example where they are subject to attack because of hatred stoked by online misinformation.

For AFP, new technologies therefore pose risks and benefits in terms of accountability and fair trial rights guarantees. Organisations such as Forensic Architecture[24] and Bellingcat[25] have used open source data and digital technologies to investigate human rights abuses, including those allegedly carried out by AFP. While these technologies may be used to hold AFP accountable, they may also be useful in providing evidence to exonerate AFP and to provide exculpatory evidence to guarantee the right to a fair trial when AFP face allegations of misconduct.

Mobile phones and other personal devices gather large amounts of information from their users which may include personal contacts, photos and correspondence as well as geo-location data and intimate health data. The increasing use of "digital strip searches" in the wider criminal justice and security system[26] may also pose a risk to the rights of AFP where such practices occur in the military context. A particular area of concern is the use of such tactics to gather extensive personal data on individuals reporting sexual assault and rape. This practice can undermine the dignity and violate the privacy of AFP reporting such incidents and may result in a reduction in the incidence of reporting which, in turn could limit efforts to tackle problems of sexual assault in the military. This could have implications for the positive obligation to protect AFP from inhuman and degrading treatment.

[23] Deepfake satellite images pose serious military and political challenges | Engadget

[24] Investigations ← Forensic Architecture (forensic-architecture.org)

[25] bellingcat - the home of online investigations

[26] https://shame.bbk.ac.uk/blog/a-digital-strip-search/

The use of digital technology in evidential trails for accountability is, therefore, potentially beneficial for AFP while there is a significant risk of falsified "evidence" with the increasing ubiquity of deepfakes and similar technologies and a risk that victims may be subjected to ill-treatment through the scale of information available on them in their digital devices.

Conclusion

New technologies can both enhance and threaten the human rights of armed forces personnel. Digital technology reaches into all aspects of the lives of AFP including their experience of warfare and combat, their personal relationships, employment records, health and reputations. Careful consideration should be given when devising policies, law and regulations relating to digital technologies in the context of the military. In some cases a balancing of rights is required – e.g. privacy and freedom of expression may be restricted to ensure national security, protection of right to life and the rights of others etc. But in cases involving absolute rights such as the right to freedom of thought or the prohibition on inhuman and degrading treatment and punishment, clear guidance needs to be drawn up to ensure there is no interference with these rights.

Careful consideration of the human rights of AFP is required to avoid unintended consequences in emerging technologies when they are at the research stage and when deployed in military contexts. The impact of BCIs designed to enhance performance, for example, should be considered holistically including long term consequences and the impact of extended periods of military service on individuals. Psychological impacts should be considered in relation to potential human rights implications as well as physical impacts.

The way data is collected and stored is extremely important for the safety and privacy of AFP. Policies and legal guidance on the collection of biometric data in particular should take account of the significant risks of information being leaked or misused. But data also provides opportunities for accountability that should be explored.

There is a degree of crossover between military technology developments and consumer technology developments as well as increasing use of consumer technology by AFP which may have consequences for their human rights, either through their use or limitations on their use. Broader digital rights concerns regarding privacy, freedom of expression and opinion and freedom of thought are equally relevant to AFP and policies should be designed to protect the digital rights of AFP in their particular context drawing on experience from the wider field of digital rights.