Regulating Military Applications of Cyber Enhancement of Human
Conference Summary

A conference entitled Regulating Military Applications of Cyber Enhancement of Humans was organized at the Hebrew University of Jerusalem by the Federmann Cyber Security Center on the 17th and the 18th of February 2019, in collaboration with Johns Hopkins Applied Physics Lab and Essex University School of Law. The goal was to adopt a multidisciplinary approach on the topic of enhancement through brain-computer interface (BCI), and to bring together experts in medicine, law, computer science, and engineering.

Some opening comments were made on the general challenges brought by these new technologies: the possible irreversibility of BCIs, access to and use of information recorded by digital means, the degree of responsibility for crimes committed by "remote controlled" individuals – and lawyers' limited understanding of technical aspects.

The first panel highlighted the bioethical aspects of BCI technologies.
It was underlined that cognitive enhancement has attractive and unattractive features. Supporters of enhancement favor the ability to have unlimited power over cognitive evolution (the idea of "reasoned argument,") whereas opponents see a danger in diluting authentic humanness (the idea of "giftedness.") As of today, many arguments can be advanced for and against BCIs and the use of bio-algorithms. For instance, spheres of empathy could expand, but big data algorithms that can monitor and understand my feelings much better than we can could also emerge, while authority would shift from humans to computers, leading to the disintegration of free will. The bio-ethics of cybernetics thus needs to be framed, and the question now is how to use BCI to maximize benefits and minimize harms while recognizing the material constraints on human cognition. In any case, the somatic embodied perspective should be taken into account.

Deep-brain stimulation (DBS) technology was then explained as an illustration of the benefits of BCI. Some issues exist with this technology, as revealed in the case of patients affected by Parkinson disease. For instance, few people are eligible for DBS, any infection or bleeding in the brain is a serious concern, patients are afraid of surgery, and the surgery is expensive. The development of this technology has met with some success (automatic navigation to DBS targets), but some dreams remain unattained (closed loop DBS for Parkinson disease) or have

encountered serious difficulties (understanding and alleviating schizophrenia through closed-loop DBS). In conclusion, it is too early to use this technology for soldier enhancement, but DBS could help people to live better.

A second panel addressed the state of Science in BCI, touching on its "good," "bad," and "ugly" aspects. The good aspect is that we can control devices by thoughts (signal acquisition – signal processing – command – feedback). A major goal is to improve the quality of life of patients with severe neuromuscular disorders (ALS, stroke) and the aging population. The technology is evolving ("dry" and "wet" EEG – i.e. requiring gel or not) and bringing BCIs to the consumer. "Active" and "passive" BCIs have also emerged: Active BCIs focus on real-time control of external devices, while passive ones focus on monitoring brain activity over longer timespans. The latter can provide biomarkers to assist in the diagnosis and treatment of patients with epilepsy, ADHD, autism, and other conditions. They can warn patients with epilepsy of an upcoming seizure and promote neuro-wellness (by monitoring stress levels, cognitive workload, and drowsiness). This finding could have military applications: monitoring the brain activity of fighter pilots could allow a warning system related to loss of consciousness and spatial disorientation. There is also a "bad" aspect, however, namely the security threat. While current technology enables brain stimulation for treating disorders and improving cognitive function, it could also be exploited to create brain damage. Finally, there is an "ugly" aspect. BCI devices could be used to extract unconscious interests and emotional reactions, which could serve for neuromarketing. In conclusion, BCIs are going to affect our future and may have military applications, raising issues related to privacy and autonomy. However, in the near future, there is no need to worry about brain hacking.

It is also possible to use BCIs to examine the mutual learning of brains and machines. Experiences with monkeys show that they are able to move a ball on a screen thanks to brain data within one minute of training. Activity of neurons in the motor cortex is dynamically adapted from the "movement state," warping into a new neuronal state-space: "BCI State." In a nutshell, when BCI is activated, the activity of the local circuit reaches a new neuronal state, adapting to the BCI state. In the future, BCIs could rely on the direct modulation of brain activity.

A third panel discussed the regulation of the experimental phase of human enhancement. Actually, there is no specific regulation about human enhancement in this context, which means

that the more general framework applicable to research on humans is relevant. Accordingly, free consent must be obtained from subjects, while vulnerable persons (children, pregnant and breastfeeding women, and persons deprived of liberty) can only take part in therapeutic research when there is a specific benefit. However, this does not mean that any type of experiment can be carried out on healthy subjects: trials must meet the proportionality test (risk versus benefit). Usually, healthy subjects may only be exposed to a minimal risk. International humanitarian law was then raised, and its analysis reveals that experiments on foreign protected persons (prisoners of war and civilians in the occupied territories) are usually prohibited. Exceptions exist when justified by the medical treatment, or state of health of the person and conducted in accordance with "generally accepted medical standards." Another problem comes with experiments carried out by armies on their own soldiers. Soldiers could indeed be forced by their hierarchy to take part into experiments, or be tempted to do so to avoid being sent to the battlefield. Unfortunately, no clear answer has been provided by human rights bodies on this issue, and it is conceivable that arguments could be made that the benefit for the society or on the battlefield should justify a higher risk (but not any risk), if the consent of the soldier is obtained.

A fourth panel focused on agency and accountability.
The definition of enhancement was discussed. This raises different questions: What is the object of improvement? What do we mean by improvement of capacities? What technologies should be considered enhancement technologies? What is the point of enhancement debates in the military and security context? The influence of BCIs on autonomy was then tackled, with respect to three dimensions of autonomy: decision-making capacity, authenticity, and the relational dimension. The influence of the type of BCI involved on these criteria was then analyzed: BCIs that merely read/interpret brain activity; BCIs that read and modulate brain activity in such a way that agents' minimal decision-making capacity is, at least temporarily, undermined; BCIs that read and modulate brain activity in such a way that decision-making capacity is not undermined.

The issue of enhancement and moral responsibility was then considered. For instance, what happens if a soldier takes an "obedience pill"? What if, based on his enhancement (e.g. a bionic eye), a soldier commits a war crime he would not have committed without this enhancement? The importance of distinguishing between causes (events that make things happen) and conditions (that allow another event to cause a certain effect) was also highlighted.

The security experts then made a number of observations. With respect to international humanitarian law, it was underlined that some weapons were prohibited because they (or their effects) generated a particular aversion (such as laser weapons causing permanent blindness). Could embedded BCI implants also follow this path? Can we overload them? Do we want to go this way? Do we want to risk permanent brain damage to soldiers? The rights of soldiers were also evoked; they may indeed be considered "citizens in uniform" who still enjoy human rights. Consequently, being enhanced does not remove them from the family of human beings. Yet BCIs bring new challenges: for instance, in terms of individual accountability. If soldiers become "puppets," they would be eligible for a defense based on their lack of control over their own actions. But most crimes need to be connected with knowledge and intent. How do we prove these elements, knowing that a large quantity of information is processed when someone is connected to a BCI?

The cybersecurity vulnerabilities of BCIs were also discussed. It is necessary to understand that vulnerability is part of the "game." Once an attacker finds a vulnerability, he attacks. This is how brain DOS or damage could appear. There is also the possibility to steal information from the interfaces (for instance, related to soldier training). BCIs are dangerous in a way: we must assume that the system is vulnerable and will be attacked. It is thus necessary to consider whether we really want to develop military uses of BCI.

Regulation was finally tackled, along with the question whether innovation and protection are conflicting. Different questions must be considered: What is new? What is different? Is BCI a digital disruption? And in what sense? Is it going to revolutionize how people think? It was underlined that it is necessary to estimate the potential adverse effects (critical or low), the potential positive effects (low or high), whether no governing rule or strong governing rules are required, the degree of innovation inhibition, and the degree of competition with non-regulated regions. In addition, one has to wonder whether existing legal frameworks sustain new risks presented by BCIs: brain hacking for personal data collection, discrimination and exclusion, identity theft, physical and psychological harm. It is also necessary to identify the most suitable form of regulation: government enforcement, public regulatory bodies, industry standards and codes, and internal regulatory bodies. A final question is whose rights should be protected – and from whom?