

EDITORIAL PREFACE: ETHICS IN CYBERSPACE

Dear Readers,

We are proud to present to you the 10th issue of the *Cyberpolitik* Journal. It is a great honor for all of us to continue our journey that we started five years ago without interruption. Day by day the interest in this field is growing and we get more and more manuscripts. As the digital world grows every day and every second, new developments and new technologies emerge, we are trying to read and understand this area within our limitations.

This volume deals with a number of topics ranging from social contract in cyberspace to digitized banking system, from China's cybersecurity strategies to Pakistan's policies. There are also rich contents in this issue and researches that will increase the question marks in our minds. But in this brief discussion, I would like to discuss the importance of cyber ethics in cybersecurity.

This year we have concluded the fourth Istanbul International Bosphorus Conference on Cybersecurity, Cyberpolitics and Social Sciences. I present on the need for cyberethics. Here is the summary of my presentation.

Cyberspace is a new man-made domain that has different characteristics than physical domains. Therefore, it requires some new way of behaving that might be challenging with the traditional ones. Cyberspace is also an anarchic domain – no central authority- where numerous threats emerge. Since there is no authority providing an order and peace it is quite difficult to have safe space. There are some cybersecurity strategies, policies, products, programs and protocols but all these means are unable to provide a real security in cyberspace. The only way to provide free and safe cyberspace is ethical behavior of the users – individuals. And the method to equip the users with ethics is a rights-based education.

Need for a Cyber Ethics?

Cyberspace has some unique characteristics that make cybersecurity difficult. The anarchic nature of cyberspace, encryption, unanimity, identity flexibility, dominance of private companies, empowerment of individuals, being a global network, no borders and distance in the sense we understand and existence of malicious codes. As a result of these unique



characteristics individuals behave differently in cyberspace as compare to physical spaces. Hence more, each of these features poses different security challenges. Thus, dealing with cybersecurity is quite a complicated issue. Despite the emergence of new technologies, cybersecurity products, cybersecurity policy and strategies it is almost impossible to create a safe and free cyberspace.

Hackers with bad intentions (black hat hackers) are capable to find new ways to overcome with the measures developed. The only way to overcome security issues in cyberspace is to educate and led users to behave ethically in cyberspace. But it is impossible to have all users – for today it is almost 4.8 billion – behave ethically. Despite all these deficiencies training users in ethics is the only way for safer cyberspace.

Ethical Problems in Cyberspace

There are numerous ethical problems in cyberspace. Monopoly of big-tech companies that try to use and misuse our personal data; robotization of human being; hacking of human brain; independent thinking of artificial intelligence (AI), usage of block chain technology in illegal activities, unauthorized access to personal data, sensitive information and web-sites are a few of them.

First of all there are big-tech companies who are monopoly in cyberspace and thus benefit from some control over users data and freedoms. Google, Twitter, Facebook, Instagram, Microsoft, Cisco, IBM, Apple have a huge amount of personal data from all over the world. They impose their roles on everyone because there are no strong companies to compete with them. This situation poses a real threat. They can misuse our data or limit our human rights and freedoms online. They can strongly violate our right to privacy or freedom of speech or freedom of information. As individual we have no power to restore or no international legal regulations to limit these companies.

Secondly, there is a huge literature discussing what if AI goes beyond the codes and act independently? What if AI thinks by itself and conduct a war against human beings? What is AI come close to human beings etc. But there is relatively few studies discussing robotization or mechanization of human being. There are many indicators showing the mechanization of human being in sci-fi TVseries Black Mirror. And this sci-fi is not far away from us. We need



to discuss these tendencies, because if happens it will be disaster for human beings. Since such happening will be one of the biggest ethical challenges by cyberspace to humanity.

Thirdly, related with the second point is the physical hacking of human brain. There are some researches focusing on the possibility of such hacking brain. They war the humanity to stop this and take measures from now to prevent it happens. They call for forming international treaties that protect human psychological and mental integrity. Otherwise, it will be too late and we will lose our humanity forever. That is one of the biggest threat to humanity and also one of the most risky ethical problems posed by cyberspace.

Fourthly, is the independence thinking of AI. To what extend we should let AI to think independently? In case they think and act independently what is going to happen? What sort of ethical problems humanity is going to face with? These questions need to be answered.

Finally, what are the ethical problems we are going to face with the emergence of new technologies such as block chain technology, bid data, clod computing, super computers etc? Each of these technologies will bring new challenges for us. For example, block chain technology is important for anonymity and cybersecurity. But what will happen if it is used in illegal activities? Since it is anonymous and impossible to remove it what are we going to do in case of an illegal action take place? For example, if there are some wrong or fake news about an individual despite the existence of many different procedures, it is possible for s/he to remove them from cyberspace either by apply to the relevant company or via judicial processes. But in block chain technology that is quite impossible. Since it is anonymous there is no responsible entity to apply to and also technically it is not possible.

There are so many other ethical issues in cyberspace. Among them are malicious codes, social engineering, phishing scams, unauthorized access to computers, unauthorized modification of data held on computers and on computer systems, cyber bullying, cybercrimes, illegal online trade activities are just few of them. There are many challenges but what are the solutions?

Some Recommendations

There are different proposals, approaches and models for overcoming ethical problems in cyberspace. Some codes of conducts are developed by NGOs and some proposed by academicians. Information society of the 21st century needs to find a right way to go further.



We need to develop coherent ethical values for cyberspace. Some are equality, freedom, attention, participation, sustainability and responsibility.

Akyesilmen (2018) proposes a rights-based model for ethical cyberspace. It is a rights-based digital citizenship education. That is a peace education, human rights education and a kind of education of ethics. Called *Ethics Phor Peace* Model.

Ethics Phor Peace Model has two meaning. On one hand it implies that there is only one way for a real cybersecurity and that is ethics. On the other hand Ethics phor Peace corresponds for some human rights values that users need to acquire and apply them online. Therefore, the *Ethics Phor Peace* corresponds to Equality, Time, Health, Information, Communication, Security, Participation, Human Right, Opportunity, Responsibility, Privacy, Empowerment, Accountability, Creativity and Empathy. The details of each concept will be given in my presentation on ethics in cyberspace.

Cyberspace has brought about many new ethical challenges that we need to overcome for a peaceful and free domain. The nature of cyberspace is prone to offence. Thus it is hard to provide security. The only way to have a safe cyberspace is ethics. Therefore, the users need education of ethics and human rights for a free and safe cyberspace.

Nezir AKYEŞİLMEN, Ph.D

Editor-in-Chief

