DIGITAL POLICY INSTITUTE - MILLENNIUM 3000 LADISLAV BOLDI



CYBER SUMMIT ON FIGHT AGAINST DISINFORMATION - EU - 2023

A historic meeting of EU Member States to approve the activation of the EU Action Plan - 2023, to fight disinformation together and to protect freedom of speech.

CYBER SUMMIT ON FIGHT AGAINST DISINFORMATION - EU - 2023



"The Cyber Summit on Fight against Disinformation - EU - 2023 is the most important summit over the past 100 years."

Contents

Introduction	3
Chapter 1 WEBSITE - CYBER WEAPONS OF MASS DESTRUCTION	5
Chapter 2 SOCIAL TERRORISM - A THREAT TO THE DIGITAL CIVILIZATION, WHICH CONSISTS OF CITIZENS OF ALL NATIONS1	1
Chapter 3 SOCIAL VIRUS - A KILLER FOR HUMANITY IN THE DIGITAL CENTURY1	8
Chapter 4 THE DIFFERENCE BETWEEN A DISINFORMATION SPREADER AND A SOCIAL TERRORIST IS NOT ONLY POLITICAL, BUT ALSO SOCIAL AND LEGAL2	
Chapter 5 DISINFORMATION - CYBER-AGGRESSION - CYBER-HATE - CYBER-BULLYING THREATEN CHILDREN MOST OF ALL2	9
Chapter 6 DISINFORMATION BURIES DEMOCRACY3	4
Chapter 7 CYBER-POLICE - EU4	1
Chapter 8 CYBER-POLITICS - AN INTEGRAL PART OF THE NEW DIGITAL WORLD ORDER4	4
Chapter 9 DWO - DIGITAL WORLD ORGANIZATION - THE NEW WORLD LEADER IN CYBER-FUTURE	9
Chapter 10 THE DIGITAL WORLD ORGANIZATION AND THE NEW DIGITAL WORLD ORDER5	6
Chapter 11 DIGITAL WORLD ORGANIZATION - BUILDER OF DIGITAL PEACE AND PROTECTOR OF DIGITAL CIVILIZATION5	9
Chapter 12 ORGANIZATIONAL STRUCTURE OF THE DIGITAL WORLD ORGANIZATION	
PRESIDENT OF DWO6	6

Introduction

DISINFORMATION WEBSITES AND SOCIAL NETWORKS ARE BECOMING CYBER WEAPONS OF MASS DESTRUCTION!

The international NGO Digital Policy Institute - millennium 3000 proposes that EU member states adopt two new laws for the digital age - the Law on Combating Social Terrorism and the Status of Cyber Danger to the State, as disinformation websites and social networks are becoming cyber weapons of mass destruction that threaten citizens' lives and health, national security and principles of the rule of law.

For the first time in history, citizens are living in two worlds (real and virtual) at the same time, but they no longer feel safe in either world.

But the situation is far worse than politicians, the media, police and intelligence services are willing to admit, which is why the Digital Policy Institute - millennium 3000 is proposing that the government passes two key laws for the digital age, in which up to 80% of all threats will come from the virtual world:

- Law on Combating Social Terrorism
- Status of Cyber Danger to the State

If people are unable to tell the difference between lies and truth because of misinformation, this is the highest level of threat to human life and health, national security and principles of the rule of law.

The spread of misinformation is a major cause of conflict in the world, giving rise to violence, injustice, tyranny, inhumane treatment, persecution, discrimination, political, social, economic and energy crises, quarrels, fear, mistrust, revenge, cyber-attacks, cyber-bullying and cyber-aggression, and hatred, which is spreading from the virtual world to the real world faster than COVID-19.

One of the most feared threats in the history of mankind is the social war that citizens wage on social networks among themselves, out of anger and hatred.

But anger and hatred are not the only causes of social war, they also include bad political decisions that lead to people venting their anger on social media in the form of hateful comments that create security and social tensions in society and end in increased aggression and hatred.

Another of the many causes of the social war that citizens wage among themselves on social networks is the fact that millions of people today live in a harmful social environment, not only in

the real world, but also in the virtual world, where a billion new pieces of misinformation appear every second, literally burying the hope for a better future.

The Cyber Summit on Fight against Disinformation - EU - 2023, presented to the EU member states and the European Commission by the international NGO Digital Policy Institute - millennium 3000, is a hope for humanity and for planet Earth, and the sooner it is organized, the sooner it will ensure the protection of the life and health of citizens and security, social, economic, energy, ecological and legal stability between people, nations and continents.

Chapter 1

WEBSITE - CYBER WEAPONS OF MASS DESTRUCTION

Disinformation websites and social networks have become cyber weapons of mass destruction through which hostile countries and cyber threat actors spread misinformation, anger, chaos, revenge, fear, distrust and hatred, threatening human lives and health of citizens, national security and principles of the rule of law.

Due to websites that social terrorists use as cyber weapons of mass destruction (disinformation websites and social networks), citizens and especially children face indescribable suffering (social terrorism - cyber-bullying, cyber-lynching, cyber-defamation, violence in schools and at home, blackmail, intimidation, social deprivation, depression, panic attacks, personality disorders, social phobias, trauma, health problems, self-harm, suicidal tendencies, fear of people, running away from home, humiliation, discrimination, broken family, interpersonal and virtual relationships, total breakdown of social infrastructure, a mentally destroyed nation with no future, crippled security and social policies inapplicable to the digital century, radicalization, extremism, nationalism, etc.).

The best way to prevent the spread of disinformation that threatens human lives, security, social, economic, energy, environmental and legal stability among people, nations and continents, and principles of the rule of law, is to first find the causes.

There are as many reasons and motives why people spread misinformation through modern and information technologies as there are stars in the sky, but the main ones include pain, despair, hopelessness, health or social handicap, disappointment, failure, human misfortune, anger, fear, poverty, mistrust, revenge, hatred, power or economic interests, and last but not least, the fact that almost no one is able to distinguish lies from truth anymore.

Similarly, people who read disinformation websites because they have had bad experiences with the media, which they consider to be instruments of power, lose trust in them and prefer to look for the truth where they think they will find it.

The spread of misinformation is leading the world into the worst war in human history, fought between people on social media, not only because of anger and hatred, but also because of bad political decisions that are destroying their lives.

Because of bad political decisions, people vent their anger on social media in the form of hateful comments, 95% of which are misinformation.

The problem is that the citizens are already in such a difficult situation that they are unable to distinguish between lies and truths, fear for their own future and growing distrust, whether towards the media, the state, politicians, authorities, public administration, political, social, economic and legal systems, which causes feelings of disappointment, fear, despair and hopelessness.

The spread of disinformation has a devastating impact on human life and health, security, social, economic, energy, environmental and legal stability among people, nations and continents, and the principles of the rule of law.

The fight against disinformation is primarily a global threat that must be addressed not at the national but at the global level, because the spread of disinformation through modern information and communication technologies leads to conflict situations not only in the real but also in the virtual world, which give rise to cyber threats and crimes, such as social terrorism, social war, cyber-terrorism, etc., and security and social tensions between people, nations and continents.

If social terrorists spread misinformation, anger, chaos, revenge, fear, distrust and hatred, it is not the fault of disinformation websites, or social networks, or Russia and China, but of politicians who are unable to build a trustworthy political, social and legal environment for citizens, in which it is easy to distinguish the truth from disinformation.

The problem is that there are more and more disinformers entering politics, and if they manage to come to power through legitimate elections, not only civil society is at risk, but also security, social, economic, energy, ecological and legal stability among people, nations and continents, and principles of the rule of law.

It shows that democracy lacks key security safeguards that no country can do without in the digital age, and therefore new global measures are needed to prevent threats and crimes committed in cyber-space, as they threaten both worlds (real and virtual) simultaneously.

The power and economic interests of politicians are another cause of the spread of misinformation, which citizens share and identify with because they cannot distinguish between lies and truth.

The influence of politicians has a profound impact on citizens, whether positive or negative, and when politicians spread misinformation through modern information and communication technologies, it is they who create conflict situations that lead to a sharp increase in security and social tensions in society.

But how to explain to politicians and citizens not to be influenced by disinformation websites and not to spread disinformation that puts not only civil society but also social, economic, energy,

ecological and legal stability among people, nations and continents and principles of the rule of law at risk?

The member states themselves probably had no idea of the destructive power of social terrorists who spread misinformation, anger, chaos, revenge, fear, mistrust and hatred.

The international NGO Digital Policy Institute - millennium 3000 is sounding the alarm and proposing to hold the first ever European Cyber Summit on Fight against Disinformation, where it wants to propose to EU member states to adopt two key laws designed for the digital millennium full of cyber threats:

- Law on Combating Social Terrorism
- Status of Cyber Danger to the State

But if EU member states do not adopt new security measures in time, as proposed by the international NGO Digital Policy Institute - millennium 3000 in its Action Plan - EU - 2023, then Europe will experience first-hand the destructive power of social terrorists who threaten by spreading misinformation, anger, chaos, revenge, fear, distrust and hatred:

- lives and health of citizens in both worlds (real and virtual) simultaneously,
- rights and freedoms in both worlds (real and virtual) simultaneously,
- security, social, economic and legal stability among people, nations and continents,
- an influential and dignified position of the EU member states in global politics and international relations,
- national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- a dignified position for the EU member states in a globally competitive environment,
- national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and also includes some functions, locations and organizations that are not critical to the maintenance of essential services, but which need protection because of the potential danger to the public),
- social capital (disrupted social relations lead to the destruction of the nation),
- cyber-economy, on which the national and global economy is existentially dependent,
- digital identity of the citizen homo digitalis,
- environment, including animals (includes all living and non-living things occurring in nature; it is a system composed of natural, artificial and social components of the material world that are or may be in constant interaction with the object under consideration).

From the spread of misinformation, anger, chaos, revenge, fear, mistrust and hatred are born threats and crimes that are committed in both worlds simultaneously and include in particular:

- social war,
- aggression,
- harming,
- injustice,
- social terrorism,
- incitement to hatred,
- bullying,
- social virus,
- state terrorism,
- animal cruelty,
- **cyber murder** (a cyber-murderer is a person or entity that spreads rumors of hatred, racism, terrorism, bullying, aggression, lynching, extremism or misinformation that cause citizens to take their own lives; this is the completed crime of cyber murder),
- **cyber-defamation** (cyber-defamation is information that is untrue or highly distorted, and the goal of perpetrators of social terrorism is to provoke hatred and hostility towards victims, damage their reputation and disrupt social relationships; cyber-defamation is one of the most widespread and feared global threats of the digital age, causing citizens around the world to face death, health, financial or personal harm),
- **cyber-hate** (the spread or promotion of cyber-hate threatens the security, social, economic and legal stability between people, nations and continents, and citizens face death, health, financial or personal harm because of it),
- **cyber-racism** (cyber-racism is the vilification of the human race, ethnic groups, national minorities, and citizens around the world face death, health, financial or personal harm because of it),
- cyber-bullying (cyber-bullying is harassment, verbal attacks, threatening the victim, through modern information and communication technologies; online threats, aggressive or abusive texts, tweets, posts or messages, as well as posting personal data, pictures or videos intended to hurt or embarrass someone else are included),
- cyber-perversion (cyber perverts pose a high security threat to society by producing,
 distributing, sharing or promoting perverse, disgusting and harmful content on the Internet
 that endangers life and health, such as videos of crimes against humanity, cruelty to
 human beings or to living beings, thus fulfilling the elements of the particularly serious
 crime of supporting and promoting social terrorism; cyber-perverts threaten the social
 health of society, on which the mental and physical health of the individual is existentially
 dependent),
- **cyber-aggression** (social terrorism can be defined as verbal assault, attack, insults, tantrums or threats that result in death, health, financial or personal harm to citizens),

- cyber-lynching (millions of citizens around the world are shamed and humiliated on social networks and face death, health, financial or personal harm because of this brutal and insidious pressure),
- trolling (is internet slang for situations that deliberately seek to stir up arguments, conflict
 and hostility in an online social community and use inflammatory messages to promote
 themselves in order to provoke emotional reactions and disrupt otherwise peaceful
 discussion),
- cyber-extremism (is a particularly serious crime, as it is characterized by the dissemination
 of political or ideological attitudes, which perpetrators of social terrorism use to threaten
 not only an individual or a group, but above all the state, and are also attributed with
 violating rights and freedoms, including the basic principles of the constitutional order of
 the rule of law),
- **cyber-disinformation** (is false or unverified information (lies, fake news, manipulation of public opinion, alarmist messages, propaganda, etc.) that causes citizens to face mortal, health, financial or personal harm because they are unable to distinguish lies from the truth in time),
- **cyber-dictatorship** (is one of the most feared global threats in the digital century, because of which the digital civilization faces psychological terror, injustice, discrimination, bullying, etc. from cyber-dictators, politicians, some public media that apply media manipulation, social networks, disinformation websites, cyber-terrorists and cyber-criminals; unlike the current dictatorship, cyber-dictatorship is much more dangerous, because whoever controls the virtual world through disinformation websites and social networks, the one controls the real world),
- cyber-discrimination (a particularly serious crime involving unequal treatment, social
 injustice, threat to rights and freedoms, silencing, oppression, support and promotion of
 hatred against a different nationality, race and religion, obstruction or denial of the
 expression of a different opinion that is not contrary to the constitutional order of the rule
 of law, intimidation, threats, dehumanization of race and human dignity),
- **cyber-paraphilia** (social terrorism can be defined as the criminal behavior of a paraphiliac who threatens the lives and health of citizens or their safety and privacy because of his/her sexual disorder),
- **fake account** (setting up fake accounts to support and promote social terrorism or to commit cyber-crime is considered a particularly serious crime),
- cyber-cannibalism (cyber cannibals scour the web-blogs, forums, anywhere personal
 information about the victim can be found looking into the deepest recesses of life,
 literally eating away at people's privacy, revealing all secrets and engaging in targeted
 attacks in search of the human body).

To win the fight against disinformation, it is therefore necessary to first defeat social terrorism, which is the main cause of threats and crimes committed in the virtual world.

The Cyber Summit on Fight against Disinformation - EU - 2023, presented to the EU member states and the European Commission by the international NGO Digital Policy Institute - millennium 3000, will contribute to the unification of rules and methodological approach in the fight against threats and crimes committed in the virtual world, with the aim of ensuring:

- protection of life and health of citizens in both worlds (real and virtual) simultaneously,
- protecting rights and freedoms in both worlds (real and virtual) simultaneously,
- security, social, economic and legal stability among people, nations and continents,
- protecting the influence and dignity of the EU member states in global politics and international relations,
- protecting the national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- protecting the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- protecting the dignity of the EU member states in a globally competitive environment,
- protecting the national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- protection of social capital (disrupted social relations lead to the destruction of the nation),
- protecting the cyber-economy on which the national and global economy existentially depends,
- protecting the digital identity of the citizen homo digitalis,
- environmental protection, including animals (includes all living and non-living things occurring
 in nature; it is a system composed of natural, artificial and social components of the material
 world that are or may be in constant interaction with the object under consideration).

Chapter 2

SOCIAL TERRORISM - A THREAT TO THE DIGITAL CIVILIZATION, WHICH CONSISTS OF CITIZENS OF ALL NATIONS

www.socialniterorismus.cz www.socialniterorismus.eu

What is cyber-terrorism?

Cyber terrorism is the collective name for terrorist attacks on computers, mobile phones ('information electronic network structures'), critical infrastructure, etc.

What is social terrorism?

Social terrorism is the collective name for threats and crimes committed in the virtual world that threaten human life and health, human rights and freedoms, and intimate (personal), moral, social and spiritual integrity.

In most member states, the Cyber Security Agency protects computers, mobile phones, critical infrastructure etc. from cyber-terrorist attacks.

However, no one, no cyber security authority, protects citizens from attacks by social terrorists who create conflict on social media by spreading misinformation, anger, fear and hatred.

Democracy appears to lack key security safeguards that no country can do without in the digital age, and new global measures are needed to prevent threats and crimes from the virtual world that threaten both worlds (real and virtual) simultaneously.

According to the Institute of the Academy of Sciences of the Czech Republic (AV-CR 26.01.2022 - Ref. 04/22), the use of the word 'Social Terrorism' is fully in line with the meaning that the Policy Digital Institute - millennium 3000 explains on its website, i.e. that social terrorism represents threats and crimes being committed in the virtual world.

The definition of 'social' is related to concepts such as social networks, social activities in the real or virtual world, social contact, social relationships, social norms, social problems, social conflict situations, social threats, social health, social deviance, etc.

The definition of 'terror' is related to concepts such as harming, violence, tyranny, crimes against humanity committed in the real or virtual world, inciting or spreading hatred, threats, intimidation, bullying, injustice, racism, discrimination, terror, social threats, etc.

'ism' is a suffix, originally derived from the ancient Greek suffix -ισμός (-ismόs), in the case of social terrorism, it refers to socially undesirable behavior in the virtual world in which social terrorists threaten digital civilization, which is made up of citizens of all nations, by spreading misinformation, anger, fear, mistrust and hatred, which give rise to crimes against humanity (war, tyranny, terrorism, racism, injustice, discrimination, bullying, etc.).

When a natural or legal person or a foreign government-sponsored group of cyber threat actors threaten a state and its citizens by creating conflict situations through modern information and communication technologies and building a socially harmful environment with the aim of causing social unrest in the country by spreading disinformation, chaos, fear, anger, distrust and hatred, it is an act of social terrorism and social terrorists in such a case are threatened with exceptional punishments, because by their undesirable (criminal) behavior in the virtual world, they threaten not only human life and health, but also national security and principles of the rule of law.

The people who carry out cyber attacks are not only cyber-criminals but also cyber-terrorists and those who create conflict situations and build socially harmful environments through modern information and communication technologies to create social unrest in the country by spreading misinformation, chaos, fear, anger, distrust and hatred are called social terrorists.

There is a diametric difference between the terms cyber-criminal, cyber-terrorist and social terrorist in terms of warning symbols for the digital age or in terms of global concepts and legal interpretation:

Cyber-criminal - uses modern information and communication technologies as a tool to commit cyber crimes (e.g.: identity theft and sensitive corporate information, including personal data, cyber-vandalism, hacking, ransomware, cyber fraud, forgery, etc.), for ransom, extortion, etc., however, cyber-criminals are motivated only by profit generation, not by political or religious ideology, or the aspiration to carry out cyber attacks on a state and its people, with the aim of overthrowing the government, threatening national security or principles of the rule of law.

Cyber-terrorist - leads an ideologically (politically, religiously) motivated attack against a state and its inhabitants (attacks on critical infrastructure, information networks, computer programs, data, detection, disruption, encryption, destruction or sabotage of systems, attacks on energy, its storage, transport and production, attacks on drinking water production or distribution systems, attacks on the government sector, public administration, politics, attacks on banking systems,

transportation, means of transport, attacks on traffic and air traffic control systems, hospitals, integrated rescue system units, military infrastructure, etc.).

Social terrorist - motivated by vindictiveness, aggression, anger, resentment, power or economic interests, as well as political ambitions, etc., uses modern information and communication technologies to create conflict situations and build a socially harmful environment, with the aim of causing social unrest in the country by spreading misinformation, chaos, fear, anger, distrust and hatred, thereby endangering not only human life and health, but also national security and principles of the rule of law.

While the EU member states are trying to protect critical infrastructure from cyber attacks, they have forgotten to protect the digital society from the spread of misinformation that threatens human life and health and national security, and from the hatred that gives birth to crimes against humanity.

Cyber attacks can significantly damage critical infrastructure, but the spread of misinformation and hatred not only destroys, it threatens:

- the essence and existence of the nation,
- the human soul (the personal, moral, social and spiritual integrity of the person, his or her social and digital identity, dignity, rights and freedoms),
- personal, professional and public life,
- family, interpersonal and virtual relationships,
- protecting life and health of citizens in both worlds (real and virtual) simultaneously,
- protecting rights and freedoms in both worlds (real and virtual) simultaneously,
- ensuring security, social, economic and legal stability among people, nations and the continents,
- protecting the influence and dignity of the EU member states in global politics and international relations,
- protecting the national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- protecting the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- protecting the dignity of the EU member states in a globally competitive environment,
- protecting the national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),

- protection of social capital (disrupted social relations lead to the destruction of the nation),
- protecting the cyber-economy on which the national and global economy existentially depends,
- protecting the digital identity of the citizen homo digitalis,
- environmental protection, including animals (includes all living and non-living things occurring
 in nature; it is a system composed of natural, artificial and social components of the material
 world that are or may be in constant interaction with the object under consideration).

There is a demonstrable difference between a cyber-terrorist and a social terrorist not only from a political or social point of view, but also from a legal point of view.

Cyber-terrorists attack critical infrastructure.

Social terrorists attack the consciousness and emotions of people by creating conflict situations and building socially harmful environments, with the aim of causing social unrest in the country, by spreading misinformation, chaos, fear, anger, distrust and hatred, thus endangering not only human life and health, but also national security and principles of the rule of law.

For the first time in history, citizens are living in two worlds (the real one and the virtual one) at the same time, but they no longer feel safe in either world.

If people are unable to distinguish between lies and the truth because of disinformation websites, this is the highest level of threat to human life and health, national security and principles of the rule of law.

To ensure the protection of citizens and national as well as global security, the EU member states need to adopt the Law on Combating Social Terrorism, and if they do so, this will be a historic event in the digital century, as crimes committed in the virtual world (brutal attacks by social terrorists, spreading misinformation, anger, cyber-aggression, cyber-bullying, revenge, incitement to hatred, etc.) threaten up to 80% of the real world, which then leads to conflict situations between people, nations and continents.

The Law on Combating Social Terrorism is one of the key weapons the EU member states must use against social terrorists before they take over the world through global media (disinformation websites and social networks).

Social terrorists are attacking not only the consciousness and emotions of citizens, but now also children, politicians and journalists, with the sole aim of creating chaos in the country and spreading distrust, fear and hatred, whether for reasons of power or economic interests, or because frustration, anger and revenge drive them to commit crime.

The world must not allow social terrorists to come to power through global media (disinformation websites and social networks).

If social terrorists come to power through the global media (disinformation websites and social networks), then citizens will face indescribable suffering and not only human lives and health or principles of the rule of law will be threatened, but also world peace and security, social, economic, energy, ecological and legal stability among people, nations and continents.

The Law on Combating Social Terrorism, together with a set of modern preventive measures proposed by the international NGO Digital Policy Institute - millennium 3000 in its Action Plan - EU - 2023, will guarantee:

- protecting life and health of citizens in both worlds (real and virtual) simultaneously,
- protecting human rights and freedoms in both worlds (real and virtual) simultaneously,
- ensuring security, social, economic and legal stability among people, nations and the continents,
- preventing the subversion of the political, social and legal systems in EU countries,
- preventing chaos and security, social and legal tensions between people, nations and continents,
- protecting the influence and dignity of the EU member states in global politics and international relations,
- protecting the national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- protecting the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- protecting a dignified position of the EU member states in a globally competitive environment,
- protecting the national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and also includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- protecting the social capital (disrupted social relations lead to the destruction of the nation),
- protecting the cyber-economy on which the national and global economy existentially depends,
- protecting the digital identity of the citizen homo digitalis,
- environmental protection, including animals (includes all living and non-living things occurring in nature; it is a system composed of natural, artificial and social components of the material world that are or may be in constant interaction with the object under consideration).

However, if the EU member states do not adopt the Law on Combating Social Terrorism in time, then the fatal failure of governments will become fully apparent, resulting in the imminent:

- threat to the life and health of citizens in both worlds (real and virtual) simultaneously,
- threat to rights and freedoms in both worlds (real and virtual) simultaneously,
- threats to security, social, economic and legal stability among people, nations and continents,
- threatening the EU member states' influential and dignified position in global politics and international relations,
- threats to the national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- threatening the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- threaten a dignified position of the EU member states in the global competitive environment,
- threats to national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and also includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- threats to social capital (disrupted social relations lead to the destruction of the nation),
- threats to the cyber-economy on which the national and global economy is existentially dependent,
- threat to the digital identity of the citizen homo digitalis,
- environmental threatening (includes all living and non-living things occurring in nature; it is a system composed of natural, artificial and social components of the material world that are or may be in constant interaction with the object under consideration).

Under the auspices of the international NGO Digital Policy Institute - millennium 3000, the e-book Social Terrorism has been published to help deter threats and crimes committed in the virtual world and to protect citizens from social terrorists whose goal is to create chaos in their country by spreading misinformation, distrust, fear and hatred, whether because of power or economic interests, or because they are driven to commit crime by frustration, anger and revenge.

The e-book Social Terrorism (all profits go to a non-profit organization for children at risk) represents a major advance in the fight against social terrorism and should therefore be incorporated by the EU member states at all levels of the education system.

For the EU member states, the book Social Terrorism provides valuable information and methodological guidance on how to work together to defeat social terrorism, stop the social war that citizens wage amongst themselves on social media out of anger and hatred, and ensure digital peace in a virtual world on which the fate of the whole world depends.

www.socialniterorismus.cz www.socialniterorismus.eu

Chapter 3

SOCIAL VIRUS - A KILLER FOR HUMANITY IN THE DIGITAL CENTURY

The social virus is spread by social terrorists through modern information and communication technologies to create social unrest in the country by spreading misinformation, chaos, fear, anger, distrust and hatred.

The social virus infection manifests itself differently for each person - someone, for example, commits a terrorist attack because they shared posts and videos that motivated them to commit terrorism, while another spreads hateful comments that create security and social tensions between people, nations and continents and turn friends into enemies.

An integral part of the Action Plan - EU - 2023, which is presented to the EU member states and the European Commission by the international NGO Digital Policy Institute - millennium 3000 in the framework of the Cyber Summit on Fight against Disinformation - EU - 2023, is the declaration of the fight not against the spreaders of disinformation, but against social terrorists who deliberately infect the digital civilization with social viruses (attacking people's consciousness and affecting their thinking and emotions), causing social unrest by spreading misinformation, chaos, fear, anger, distrust and hatred.

The difference between a disinformer and a social terrorist is not only political, but social and legal.

Just because people spread misinformation doesn't make them criminals. There are many reasons why they do so, but the main ones include personal problems and the fact that they are no longer able to tell the difference between a lie and the truth.

However, those who spread disinformation deliberately are social terrorists who, through modern information and communication technologies, create conflict situations and build socially harmful environments with the aim of causing social unrest in the country primarily by spreading disinformation, chaos, fear, anger, distrust and hatred.

The purpose of the Action Plan - EU - 2023, which the international NGO Digital Policy Institute - millennium 3000 is presenting to the EU Member States and the European Commission in the framework of the Cyber Summit on Fight against Disinformation - EU - 2023, is to declare the fight not against the spreaders of disinformation, but against the social terrorists who pose a threat:

- lives and health of citizens in both worlds (real and virtual) simultaneously,
- rights and freedoms in both worlds (real and virtual) simultaneously,
- security, social, economic and legal stability among people, nations and continents,
- an influential and dignified position of the EU member states in global politics and international relations,

- national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- a dignified position for the EU member states in a globally competitive environment,
- national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and also includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of potential danger to the public),
- social capital (disrupted social relations lead to the destruction of the nation),
- cyber-economy, on which the national and global economy is existentially dependent,
- digital identity of the citizen homo digitalis,
- environment, including animals (includes all living and non-living things occurring in nature; it is a system composed of natural, artificial and social components of the material world that are or may be in constant interaction with the object under consideration).

Once again, democracy is shown to lack key security safeguards that no country can do without in the digital age, and new global measures are needed to prevent threats and crimes committed in the virtual world that threaten both worlds (real and virtual) simultaneously.

The world has reached an impasse and, moreover, because of social terrorists, the current political, security, social, economic, energy, ecological and legal situation is so bad that open hatred is growing between people, nations and continents, turning friends into enemies.

The problem is that through social terrorists who purposefully infect digital society with social viruses, there is a deliberate occupation of cyber-space, which is home to more than 6 billion users of modern and information and communication technologies, which is a much more serious threat than a military occupation, because to occupy a foreign country in the digital century will no longer require an army or tanks or airplanes, but disinformation websites and social networks controlled by dictatorial regimes.

All the causes of cyber threats go back to a deep political past in which problems were traditionally swept under the carpet and then became the legacy of successive governments.

In the meantime, most cyber threats have swelled to apocalyptic proportions, which the world cannot cope with today, and if politicians fail to prevent the rampage of social terrorists and the spread of social beliefs in time, the whole world will face a global armed conflict within five years at the latest.

Other cyber threats posed by the social virus that have a devastating impact on the EU member states include:

- social terrorism (threats and crimes committed in the virtual world),
- social war (the worst war in the history of mankind, waged by citizens against each other on social networks out of anger and hatred),
- **cyber-disinformation** (threatening not only human life and health, but also security, social, economic, energy, environmental and legal stability among people, nations and continents, and principles of the rule of law),
- social death (most often it appears wherever politicians go in the wrong direction and cannot resolve conflict situations, e.g. high inflation, collapsing political, social economic system, growing international tensions in the world, war conflicts, violence, lawlessness, racism, terrorism, the negative influence of disinformation websites that threaten the security, social, economic and legal stability of the country, the spread of hatred on social media that causes citizens to face personal, financial, health or mortal harm, COVID-19, corruption, etc.),
- **digital depression** (which is overwhelmingly affecting interpersonal relations, most often due to hate speech, spreading through disinformation websites and social networks faster than a coronavirus, and causing security and social tensions between people, nations and continents),
- **cyber-aggression** (is much more dangerous than aggression itself, as social terrorists attack en masse, through social networks such as Facebook, TikTok, Instagram, Twitter, WhatsApp or Viber),
- **cyber-lynching** (it is an act of social terrorism in which perpetrators take the law into their own hands and spread misinformation on social media in order to stir up mass hatred against the person they are attacking),
- cyber-bullying (compared to traditional bullying, cyber-bullying is so destructive that it often
 drives citizens to commit suicide, preceded by a massive attack by social terrorists who use
 modern information and communication technologies, social networks, messengers or emails
 to commit social terrorism),
- **cyber-racism** (belongs to one of the most feared global threats of the millennium, as social terrorists spread it mainly through disinformation websites and social networks),
- **cyber-hate** (cyber-hate spread by social terrorists in the virtual world where the digital civilization, consisting of citizens of all nations, lives and works, has such a devastating effect that it can cause health or death to the victims),
- **cyber-defamation** (the goal of social terrorists is to damage the victim's reputation as much as possible or to completely disrupt the victim's life).

The aim of the Action Plan - EU - 2023, which is presented to the EU member states and the European Commission by the international NGO Digital Policy Institute - millennium 3000 within the frame of the Cyber Summit on Fight against Disinformation - EU - 2023, is to prevent the cyber

occupation of the EU member states, which no longer requires armies, tanks or planes, but disinformation websites and social networks controlled by dictatorial regimes.

Chapter 4

THE DIFFERENCE BETWEEN A DISINFORMATION SPREADER AND A SOCIAL TERRORIST IS NOT ONLY POLITICAL, BUT ALSO SOCIAL AND LEGAL

Warning

The term 'disinformer', or 'disinformation spreader' ('misinformation spreader'), will no longer be used publicly, because disinformers include citizens of integrity who spread disinformation, but unintentionally. The reason why they do so is because they are unable to distinguish the lie from the truth.

The whole world will, for political, social and legal reasons, have to replace the term 'disinformer', or 'disinformation spreader' ('misinformation spreader'), with the term 'social terrorist', who is the real criminal, unlike the citizens of integrity who spread disinformation unintentionally and only because they are unable to distinguish between lies and truth.

It would be a bad political decision to prosecute the disinformation spreaders, even though it is true that disinformation spreaders spread lies, manipulate the truth, create false or distorted news, mislead people, etc., but that still does not make them criminals, especially when the most common spreaders of disinformation include people who are actually unable to tell the difference between lies and truth themselves.

However, if the efforts of the disinformation spreaders are to deliberately create social unrest in a country by spreading misinformation, chaos, fear, anger, distrust and hatred, then they are already committing the particularly serious crime of social terrorism.

Despite the fact that millions of citizens spread (forward, share, etc.) disinformation, for example, because they cannot distinguish between lies and truth, they do not pose the same security threat as social terrorists who, through modern information and communication technologies, create conflict situations and build socially harmful environments with the aim of causing social unrest in the country primarily by spreading disinformation, chaos, fear, anger, distrust and hatred.

The intention of the Action Plan - EU - 2023, which is presented to the EU member states and the European Commission by the international NGO Digital Policy Institute - millennium 3000 within the frame of the Cyber Summit on Fight against Disinformation - EU - 2023, is to prevent social terrorists from gaining power through legitimate elections in which anyone who is legally eligible can run, regardless of political ideology or criminal history.

The Law on Combating Social Terrorism is one of the key weapons that the EU member states can adopt at the Cyber Summit on Fight against Disinformation - EU - 2023 and subsequently use against social terrorists, who are ruthlessly threatening, just to gain power through global media (disinformation websites and social networks), the following:

- lives and health of citizens in both worlds (real and virtual) simultaneously,
- rights and freedoms in both worlds (real and virtual) simultaneously,
- security, social, economic and legal stability among people, nations and continents,
- an influential and dignified position of the EU member states in global politics and international relations,
- national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- a dignified position for the EU member states in a globally competitive environment,
- national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and also includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of potential danger to the public),
- social capital (disrupted social relations lead to the destruction of the nation),
- cyber-economy, on which the national and global economy is existentially dependent,
- digital identity of the citizen homo digitalis,
- environment, including animals (includes all living and non-living things occurring in nature; it is a system composed of natural, artificial and social components of the material world that are or may be in constant interaction with the object under consideration).

The purpose of the Law on Combating Social Terrorism, as proposed by the international NGO Digital Policy Institute - millennium 3000, is not to restrict freedom of speech or to punish the spreaders of misinformation, but to prosecute social terrorists who use modern information and communication technologies to create conflict situations and build a socially harmful environment with the aim of causing social unrest in the country by spreading misinformation, chaos, fear, anger, distrust and hatred.

At the Cyber Summit on Fight against Disinformation - EU - 2023, the international NGO Digital Policy Institute - millennium 3000 wants to present a methodological approach to the EU member states for the adoption of the Law on Combating Social Terrorism.

The actual wording of the Law Draft on Combating Social Terrorism, as presented by

the Digital Policy Institute - millennium 3000, should be as follows:

Criminal Code

Section on SOCIAL TERRORISM

Status of Cyber Danger to the State

General Provisions

If disinformation websites and social networks (profile, account) are used as cyber weapons of mass destruction (to create conflict situations that arise due to the spread of misinformation, anger, chaos, revenge, fear, distrust and hatred that put citizens and the state in critical danger), then the government (National Security Council) must declare a status of cyber danger to the state.

A status of cyber danger to the state should always be declared if lives, health, national security, principles of the rule of law or territorial integrity are threatened, if the intensity of the cyber danger is significant and if it cannot be averted by standard cyber protection procedures.

If hostile countries and cyber threat actors threaten the lives and health of citizens, national security and principles of the rule of law by spreading misinformation, anger, chaos, revenge, fear, distrust and hatred, then they become social terrorists who use disinformation websites and social networks as cyber weapons of mass destruction.

In the digital age, websites (or profiles, accounts, etc.) have become a cyber weapon of mass destruction through which social terrorists spread misinformation, anger, chaos, revenge, fear, distrust and hatred, which puts citizens and the state at critical risk.

Disrupting the digital society

- (1) Anyone who creates conflict situations by spreading misinformation, chaos, fear, anger, distrust and hatred towards social network users, national, racial or religious groups, fulfils the elements of the offence of social terrorism and shall be punished for
- (2) Anyone who creates conflict situations, with the purpose of exploiting or endangering the vulnerable minds of minors, by spreading misinformation, chaos, fear, anger, distrust and hatred towards social network users, national, racial or religious groups and thereby endangers life and

health, fulfils the elements of the offence of social terrorism and will be punished for

- (3) Anyone who creates conflict situations by spreading misinformation, chaos, fear, anger, distrust and hatred towards social network users, national, racial or religious groups and thereby endangers life and health, fulfils the elements of the offence of social terrorism and shall be punished for
- (4) Anyone who creates conflict situations by spreading misinformation, chaos, fear, anger, distrust and hatred and thereby endangers national security, fulfils the elements of the offence of social terrorism and shall be punished for
- (5) Anyone who creates conflict situations by spreading misinformation, chaos, fear, anger, distrust and hatred and thereby endangers the security of the European Union fulfils the elements of the offence of social terrorism and shall be punished for

Financial support from the EU member states to non-profit organizations, policy institutes, media, etc. is unconditional, but only if the applicants present a solution, or a global project, such as the Action Plan - EU - 2023, which will contain a concrete methodological approach for successfully combating disinformation within the EU territory.

However, providing funding to non-profit organizations dealing with disinformation, political institutes or independent media that help in the fight against false content without first presenting a solution, for example the draft Action Plan - EU - 2023 to fight disinformation, is not only a bad political decision and a dangerous precedent that may cast the EU member states in a bad light for trying to financially support (corrupt) befriended media with taxpayers' money.

The efforts of NGOs, public media and social networks to combat misinformation are undoubtedly meritorious, but completely useless, because the world is literally infested with misinformation, and a billion new misinformation appears in the virtual world every second.

The aim of the international NGO Digital Policy Institute - millennium - 3000 is to help the EU member states and the European Commission fight social terrorism and protect the European Union from threats and crimes committed in the virtual world.

It is extremely important for the media to help raise global awareness of the fight against social terrorism, because only in this way can the world successfully confront social terrorists, but financial support for non-profit and international organizations, policy institutes, media, etc. can only be issued if they present their own project to combat threats and crimes committed in the virtual world.

The EU member states may not abdicate their duty to protect human life and health, national security and principles of the rule of law; they must only approach those non-profit and

international organizations, political institutes, media, etc., which put forward their own project to combat threats and crimes committed in the virtual world.

Otherwise, the member states could find themselves under suspicion (corrupt practices) of giving EU funds to be friended non-profit organizations, international organizations, political institutes, media, etc. that lobby for the interests of political parties.

The international NGO Digital Policy Institute - millennium 3000 is the only public sector organization that meets all the standards, requirements and criteria to receive EU grants for its global projects aimed at combating threats and crimes committed in the virtual world.

The international NGO Digital Policy Institute - millennium 3000 is ready to assist the European Union in protecting the digital society from threats and crimes committed in the virtual world, which unfortunately none of the EU member states has managed to do so far.

While most EU member states have established a cyber security authority to protect critical infrastructure, computers, mobile phones, etc., politicians have completely forgotten to protect their citizens from threats and crimes committed in the virtual world, which include:

- social terrorism (threats and crimes committed in the virtual world),
- social war (the worst war in the history of mankind, waged by citizens against each other on social networks out of anger and hatred),
- cyber-disinformation (threatening not only human life and health, but also security, social, economic, energy, environmental and legal stability among people, nations and continents, and principles of the rule of law),
- social death (most often it appears wherever politicians go in the wrong direction and cannot resolve conflict situations, e.g. high inflation, collapsing political, social economic system, growing international tensions in the world, war conflicts, violence, lawlessness, racism, terrorism, the negative influence of disinformation websites that threaten the security, social, economic and legal stability of the country, the spread of hatred on social media that causes citizens to face personal, financial, health or mortal harm, COVID-19, corruption, etc.),
- digital depression (which is overwhelmingly affecting interpersonal relations, most often due to hate speech, spreading through disinformation websites and social networks faster than a coronavirus, and causing security and social tensions between people, nations and continents),
- **cyber-aggression** (it is much more dangerous than aggression itself, as social terrorists attack en masse, through social networks such as Facebook, TikTok, Instagram, Twitter, WhatsApp or Viber),
- **cyber-lynching** (it is an act of social terrorism in which perpetrators take the law into their own hands and spread misinformation on social media in order to stir up mass hatred against the person they are attacking),

- cyber-bullying (compared to traditional bullying, cyber-bullying is so destructive that it often
 drives citizens to commit suicide, preceded by a massive attack by social terrorists who use
 modern information and communication technologies, social networks, messengers or emails
 to commit social terrorism),
- **cyber-racism** (belongs to one of the most feared global threats of the millennium, as social terrorists spread it mainly through disinformation websites and social networks),
- **cyber-hate** (cyber-hate spread by social terrorists in the virtual world where the digital civilization, consisting of citizens of all nations, lives and works, has such a devastating effect that it can cause health or death to the victims),
- **cyber-defamation** (the goal of social terrorists is to damage the victim's reputation as much as possible or to completely disrupt the victim's life).

The list of global projects prepared by the international NGO Digital Policy Institute - millennium 3000 to ensure the protection of the European Union against threats and crimes committed in the virtual world is extensive and includes:

- BOOK CYBER SUMMIT ON FIGHT AGAINST DISINFORMATION EU 2023,
- GLOBAL EDUCATION OF THE PUBLIC SOCIAL TERRORISM (strategy and methodology of the fight against threats and crimes committed in the virtual world),
- ACTION PLAN EU 2023 (common fight against disinformation and other cyber threats at the level of the EU member states),
- PROTECTING CHILDREN AND THE DIGITAL SOCIETY EU against threats and crimes committed in the virtual world,
- ESTABLISHING A EUROPEAN LAW ON COMBATING SOCIAL TERRORISM and also at the level of the EU member states,
- GLOBAL EDUCATION OF THE PUBLIC SOCIAL EDUCATION (digital education, digital literacy, moral literacy, social literacy, cyber-education, cyber protection against social terrorists, etc.),
- DIGITAL WORLD ORGANIZATION DWO (a new global body intended for cyber-future, the mission of which is to protect the digital civilization, which consists of citizens of all nations, from threats and crimes committed in the virtual world),
- DIGITAL CONSTITUTION DWO (the Digital Constitution guarantees the protection of life and health, including the rights and freedoms of the digital civilization, which is made up of citizens of all nations),
- CYBER-POLICE EU (a new European criminalistics authority to protect children and digital society from threats and crimes committed in the virtual world; cyber-police will also be created at the member states - EU level).

The international NGO Digital Policy Institute - millennium 3000 is ready to work with the European Commission to promote new global projects, providing not only technical assistance but

also helping the EU member states to protect digital society against threats and crimes committed in the virtual world.

The EU member states will learn about all the new global projects developed by the International NGO Digital Policy Institute - millennium 3000 to protect the European Union from threats and crimes committed in the virtual world at the Cyber Summit on Fight against Disinformation - EU - 2023.

Chapter 5

DISINFORMATION - CYBER-AGGRESSION - CYBER-HATE - CYBER-BULLYING THREATEN CHILDREN MOST OF ALL

The purpose of the Cyber Summit on Fight against Disinformation - EU - 2023 is to send a clear message to the world in support of protecting children who are most affected by threats and crimes committed in the virtual world.

For the international NGO Digital Policy Institute - millennium 3000, the protection of children in cyber-space is one of the key priorities for which it has developed the Action Plan - EU - 2023, an integral part of which is the organization of the Cyber Summit on Fight against Disinformation - EU - 2023.

Sending a clear signal to the world through the Cyber Summit on Fight against Disinformation - EU - 2023 to support the protection of children in cyber-space is a historic event for parents who have been waiting impatiently for several years for a law on the protection of children in cyber-space.

In the Action Plan - EU - 2023, the international NGO Digital Policy Institute - millennium - 3000 proposes the adoption of the Law on Combating Social Terrorism, in which article (2) clearly states: Anyone who creates conflict situations, with the purpose of exploiting or endangering the vulnerable minds of minors, by spreading misinformation, chaos, fear, anger, distrust and hatred towards social network users, national, racial or religious groups and thereby endangers life and health, fulfils the elements of the offence of social terrorism and will be punished for

There is a social war raging on social networks, waged by citizens around the world against each other for reasons of anger, revenge and hatred, and it is moving from the virtual world to the real world, and due to this destructive threat, security and social tensions are growing in society, which immediately threatens the lives and health of citizens and especially children, and the security, social, economic and legal stability of the country.

That is why the organization of the Cyber Summit - EU - 2023 on fight against disinformation is inevitable, in which it will be necessary to unify the security rules of EU member states in the following areas:

- GLOBAL EDUCATION OF THE PUBLIC SOCIAL TERRORISM (strategy and methodology of the fight against threats and crimes committed in the virtual world),
- ACTION PLAN EU 2023 (common fight against disinformation and other cyber threats at the level of the EU member states),
- PROTECTING CHILDREN AND THE DIGITAL SOCIETY EU against threats and crimes committed in the virtual world,

- ESTABLISHING A EUROPEAN LAW ON COMBATING SOCIAL TERRORISM and also at the level of the EU member states,
- GLOBAL EDUCATION OF THE PUBLIC SOCIAL EDUCATION (digital education, digital literacy, moral literacy, social literacy, cyber-education, cyber-protection against social terrorists, etc.),
- DIGITAL WORLD ORGANIZATION DWO (a new global body intended for cyber-future, the mission of which is to protect the digital civilization, which consists of citizens of all nations, from threats and crimes committed in the virtual world),
- DIGITAL CONSTITUTION DWO (the Digital Constitution guarantees the protection of life and health, including the rights and freedoms of the digital civilization, which is made up of citizens of all nations),
- CYBER-POLICE EU (a new European criminalistics authority to protect children and digital society from threats and crimes committed in the virtual world; cyber-police will also be created at the member states EU level).

Due to the threats and crimes committed in the virtual world, millions of children around the world face indescribable suffering as a result of vulnerable minds being exploited or threatened, especially by social terrorists who do not avoid anything.

As a consequence of abuse or endangerment of the vulnerable brains of minors, children experience dramatic events that are accompanied by **social deviance** (a collective term for unhealthy, abnormal and generally undesirable social phenomena, i.e. socially dangerous, negatively sanctioned forms of deviant behavior that do not conform to the moral, social or legal norms of society), triggered by social warfare:

- arguing, screaming,
- disturbed psyche,
- problems at home and at school,
- depression,
- despair,
- helplessness,
- anger, rage, fury,
- vindictiveness,
- envy,
- aggressiveness,
- hurting others, bullying, physical assault, etc.,
- escapes,
- self-harm,
- abuse of persons or animals, etc.,

suicidal tendencies.

Part of the Action Plan - EU - 2023, which is presented to the EU member states and the European Commission by the international NGO Digital Policy Institute - millennium 3000 within the frame of the Cyber Summit on Fight against Disinformation - EU - 2023, is to obtain a grant to launch a global awareness of the fight against threats and crimes committed in the virtual world and to include the new subject of SOCIAL EDUCATION at all levels of the educational system, the tribal structure of which is:

- **DIGITAL EDUCATION** (how to behave on social networks (in cyber-space) it is an innovative use of emotional intelligence, the ability to recognize in time inadequate or even criminal behavior of users of modern information and communication technologies, etc.),
- **DIGITAL LITERACY** (is the set of individual (digital) competences that an individual needs to use digital technologies safely, confidently, critically and creatively at work, in learning, in leisure and in his/her involvement in social life),
- **MORAL LITERACY** (it is about serious, honest, fair, brave, just and considerate behavior in cyber-space and in digital society),
- SOCIAL LITERACY (it is knowledge of the self, but also basic knowledge of applied psychology about human behavior and ethics; social literacy includes positive attitudes and value relationships; it is related to communication skills, cooperation skills or the ability to take responsibility for one's actions),
- CYBER-EDUCATION (traditional education will be transferred to the Internet in the cyber-future),
- **CYBER-PROTECTION AGAINST SOCIAL TERRORISTS** (the science of protecting human life and health of users of modern information and communication technologies from cyber threat actors and social terrorists).

SOCIAL EDUCATION is a universal platform designed for all levels of the education system that not only protects children, but also teaches them how to behave on social networks and how to successfully ward off threats and crimes committed in the virtual world.

The purpose of SOCIAL EDUCATION is to promote digital prevention not only in personal, professional or public life, but also in interpersonal and virtual relationships, as prevention has a key impact on:

- the essence and existence of the nation,
- the human soul (the personal, moral, social and spiritual integrity of the person, his or her social and digital identity, dignity, rights and freedoms),
- personal, professional and public life,

- family, interpersonal and virtual relationships,
- protection of life and health of citizens in both worlds (real and virtual) simultaneously
- protecting rights and freedoms in both worlds (real and virtual) simultaneously,
- ensuring security, social, economic and legal stability among people, nations and the continents,
- protecting the influence and dignity of the EU member states in global politics and international relations,
- protecting the national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- protecting the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- protecting the dignity of the EU member states in a globally competitive environment,
- protecting the national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- protection of social capital (disrupted social relations lead to the destruction of the nation),
- protecting the cyber-economy on which the national and global economy existentially depends,
- protecting the digital identity of the citizen homo digitalis,
- environmental protection, including animals (includes all living and non-living things occurring in nature; it is a system composed of natural, artificial and social components of the material world that are or may be in constant interaction with the object under consideration).

SOCIAL EDUCATION is a new universal educational digital platform which will be used in their daily lives by:

- parents (foster parents, children's homes, educational institutions, detention centers, etc.),
- schools (for all levels of the education system),
- **virtual training centers** (resocialization and retraining of persons, employees, etc.),
- public administration (resocialization and retraining in all areas of political and public life),
- public institutions (hospitals, offices, etc.),
- natural and legal persons (tradesmen, entrepreneurs, craftsmen, etc.),
- users of new technologies, of which there will be 9 billion by 2050,
- prisons (resocialization and retraining of prisoners, etc.).

Not only does the safety and protection of children depend on a new subject like SOCIAL EDUCATION, but also the following:

- protection of life and health of citizens in both worlds (real and virtual) simultaneously,
- protection of human rights and freedoms in both worlds (real and virtual) simultaneously,
- ensuring security, social, economic and legal stability among people, nations and the continents,
- preventing the subversion of the political, social and legal systems in EU countries,
- preventing chaos and security, social and legal tensions between people, nations and continents,
- protecting the influence and dignity of the EU member states in global politics and international relations,
- protecting the national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- protecting the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- protecting a dignified position of the EU member states in the globally competitive environment,
- protecting the national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- protecting the social capital (disrupted social relations lead to the destruction of the nation),
- protecting the cyber-economy on which the national and global economy existentially depends,
- protecting the digital identity of the citizen homo digitalis,
- environmental protection, including animals (includes all living and non-living things occurring
 in nature; it is a system composed of natural, artificial and social components of the material
 world that are or may be in constant interaction with the object under consideration).

The mission of the Action Plan - EU - 2023, which is being presented to the EU member states and the European Commission by the international NGO Digital Policy Institute - millennium 3000 within the frame of the Cyber Summit on Fight against Disinformation - EU - 2023, is to protect the digital society with a set of modern preventive measures, dominated by the new subject of SOCIAL EDUCATION.

Chapter 6

DISINFORMATION BURIES DEMOCRACY

Democracy, which is under attack by social terrorists who use disinformation websites and social networks as cyber weapons to create conflict situations and build socially damaging environments to create social unrest in the country primarily by spreading misinformation, chaos, fear, anger, distrust and hatred, is dying.

Democracy has been shown to lack key security safeguards that no country can do without in the digital age, and new global measures are needed to prevent threats and crimes from the virtual world that threaten both worlds (real and virtual) simultaneously.

While the EU member states are trying to protect critical infrastructure from cyber attacks, politicians have forgotten to protect democracy from social terrorists who create conflict situations and build socially damaging environments with the aim of creating social unrest in the country primarily by spreading misinformation, chaos, fear, anger, distrust and hatred.

On 9 July 2017, the European Commission received an email warning from Ladislav Boldi, the author of the book Cyber Summit on Fight against Disinformation - EU - 2023, that social terrorism threatened human life and health, the security, social, economic, energy, environmental and legal stability of the EU member states, principles of the rule of law and democracy itself, but none of the politicians took the warning seriously at that time.

At the time, the author of the book Cyber Summit on Fight against Disinformation - EU - 2023 was desperately trying to explain to the members of the European Commission that social terrorism has thousands of forms, many of which pose deadly threats to democracy.

The author of the book Cyber Summit on Fight against Disinformation - EU - 2023 warned back in 2015 that if social terrorists who purposefully spread misinformation, chaos, fear, anger, distrust and hatred of power, through legitimate elections and due to global media (disinformation websites and social networks), then democracy will face a mortal threat, because it has no defense mechanisms to prevent social terrorists from running for office.

Now the author Ladislav Boldi presents to the EU member states and the European Commission the Action Plan - EU - 2023, contained in the book Cyber Summit on Fight against Disinformation - EU - 2023, to combat threats and crimes being committed in the virtual world that threaten human life and health, security, social, economic, energy, environmental and legal stability among people, nations and continents, and principles of the rule of law.

The EU member states must hand-in-hand remedy and adopt the Law on Combating Social Terrorism, as proposed by the International NGO Digital Policy Institute - millennium 3000, to ensure the protection not only of critical infrastructure, but above all of digital society, which in the virtual world faces brutal attacks from social terrorists and has no protection from anyone.

However, in order for the Law on Combating Social Terrorism to be adopted throughout the European Union, a reform of the international order is needed to help protect both worlds (real and virtual) simultaneously.

Without any reform of the international order, the fight against social terrorism would be completely meaningless, because the risks and threats the world will face in the coming digital century would forever bury the hope for the digital peace on which the following depends:

- protection of life and health of citizens in both worlds (real and virtual) simultaneously,
- protection of human rights and freedoms in both worlds (real and virtual) simultaneously,
- ensuring security, social, economic and legal stability among people, nations and the continents,
- preventing the subversion of the political, social and legal systems in EU countries,
- preventing chaos and security, social and legal tensions between people, nations and continents,
- protecting the influence and dignity of the EU member states in global politics and international relations,
- protecting the national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- protecting the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- protecting a dignified position of the EU member states in the globally competitive environment,
- protecting the national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- protecting the social capital (disrupted social relations lead to the destruction of the nation),
- protecting the cyber-economy on which the national and global economy existentially depends,
- protecting the digital identity of the citizen homo digitalis,
- environmental protection, including animals (includes all living and non-living things occurring
 in nature; it is a system composed of natural, artificial and social components of the material
 world that are or may be in constant interaction with the object under consideration).

The reform of the international order will be the most complex and expensive process in the history of mankind, because citizens today live in two worlds (real and virtual) simultaneously, and therefore the following will be an integral part of it:

- digital world order (building a digital peace on which global security, world peace and lasting security, social, economic and legal stability between people, nations and continents depend),
- digital political system with a modern social and legal infrastructure that connects both worlds (real and virtual) simultaneously through modern information and communication technologies,
- digital declaration of human rights and freedoms and human duties that connects both worlds (real and virtual) simultaneously,
- **digitalization of power** (political power will be transferred to modern information and communication technologies and artificial intelligence),
- cyber-politics (all politics moves into cyber-space),
- **digitalization of politics** (people will be able to decide the future of their nation online via smartphones, if they are connected to a digitalized public administration),
- digital nation (in the digital century, the future of the nation depends on five key pillars, which
 are cyber-politics, cyber-security, cyber-economy, cyber-education and a digital declaration of
 human rights and freedoms and responsibilities),
- homo digitalis (a person living in the digital world (homo digitalis) is surrounded by ubiquitous and online connected screens and displays),
- **cyber-politician** (a prerequisite for entering the digital parliament should be digital literacy of MPs and members of the government in the field of cyber-politics, which they cannot do without in the digital century),
- digital public administration headed by its Presidium (the Presidium of Public Administration
 will make decisions and be responsible for activities related to the provision of public services,
 the management of public affairs at local and central level and the provision of matters of
 public interest),
- environmental peace (guaranteeing protection of the environment and animals).

The reason why reform of the international order is necessary is also that the world is entering the digital millennium, in which citizens live in two worlds simultaneously, and this new dimension of reality makes it important to ensure that the digital civilization, which is made up of citizens of all nations, is protected from the cyber propaganda of dictatorial regimes.

Today, the cyber propaganda of dictatorship regimes influences almost 5 billion users, who, because of disinformation websites and social networks, are no longer able to distinguish between

lies and the truth, and can therefore very easily elect a dictator, a manipulator of public opinion, a disinformer, a populist or an extremist to lead their country and start a nuclear war.

Political parties' agendas are not adapted to the digital age, and therefore humanity is at risk of cyber-dictators, cyber-disinformers and cyber-extremists coming to power through legitimate elections, using disinformation websites and social networks to speak to millions of citizens and purposefully create conflict by spreading disinformation, anger, fear, distrust and hatred.

There are millions of citizens in the world who are under the influence of dictatorial regimes and are influenced by their propaganda through modern information and communication technologies.

Threats and crimes committed in the virtual world threaten digital civilization to such an extent that cyber-space is no longer safe.

If digital civilization continues to face attacks from dictatorship regimes and social terrorists, then the real world, which is already dependent on the virtual world for its existence, will be in imminent danger.

The list of threats and crimes being committed in both worlds (real and virtual) simultaneously is quite a compelling reason why reform of the international order is necessary before any one of them comes to fruition.

SECURITY THREATS:

- global armed conflict,
- terrorism,
- racism,
- extremism,
- nationalism,
- neo-fascism,
- communism,
- dictatorship,
- elections (through legitimate elections, anyone can come to power dictators, oligarchs, extremists, radicals, nationalists, communists, populists, corrupters, liars and crooks, and there is no security measure to prevent them from taking power),
- organized crime,
- state bullying,
- police brutality,
- threats to national sovereignty in the real world and in the digital world.

SOCIAL THREATS:

- social terrorism,
- growing social tensions in society (caused by the spread of hatred, which gives rise to social disruption, discrimination, injustice, racism, bullying, terrorism, etc.),
- spreading hatred between people, nations and continents,

- attacks or state bullying of socially disadvantaged citizens (millions of households are
 dealing with the post-covid crisis, which has an overwhelming impact on citizens from all
 walks of life, families, individuals, sick people, pensioners, single mothers, people from
 social institutions, asylums and prisons, etc.),
- frustration, depression, security and social tensions between people, nations and continents,
- deformation of society (caused by global threats and security, social, economic and legal crisis),
- tarnishing personal and national dignity (disrespect for the nation and damaging its dignity by defamation and criminal enterprise in political and public life),
- turning people, nations and continents against each other.

HEALTH THREATS:

- threats to human life and health (spreading misinformation can also be to blame, causing citizens to face death or health harm because they are unable to distinguish lies from the truth in time),
- poor healthcare or access to healthcare (the main reasons for poor healthcare include corruption in the health sector, poor coordination of the health system, poor quality or lack of health personnel, unwillingness, unscrupulousness, lack of modern information technology and artificial intelligence that could replace physical activity in many areas, etc.).

ECONOMIC THREATS:

- disproportionate waste of taxpayer funds,
- illegal or unlawful use of public funds (squandering taxpayers' money),
- economic crimes (criminal enterprise in political and public life),
- misinformation, false promises, dishonesty with voters, populism and manipulation with public opinion (politicians trying to please voters even at the cost of a false future),
- power protectionism (political machinations with taxpayers' money),
- economic sanctions that create security and social tensions around the world,
- corruption (threatens the security, social, economic and legal stability of the country, causes social, economic and legal chaos in the country, undermines economic performance and threatens business, is behind the emergence of organized crime and tax evasion).

ENVIRONMENTAL THREATS:

• threats to life and health from global warming (causes: burning of fossil fuels, as the burning of coal, oil and natural gas produces carbon dioxide and nitrogen oxides; deforestation, as trees absorb CO₂ from the atmosphere and thus help regulate the climate; transport, which is a major producer of the greenhouse gases CO₂ and NO₂;

intensified cattle farming, as cows, as ruminants, produce large amounts of methane during digestion; the use of nitrogen fertilizers, which emit nitrous oxide; the use of fluorinated gases, e.g. in manufacture of refrigeration equipment, air conditioners and heat pumps, etc., which cause a strong greenhouse effect),

- threats to life and health caused by extreme weather events (causing severe damage to property, infrastructure and lives),
- the inability and unwillingness of politicians and companies to mitigate the climate threat (significant biodiversity loss and ecosystem collapse),
- threats to life and health caused by human damage to the environment (oil spills, radioactive contamination, etc.),
- reckless politics that is leading to global migration,
- abuse or inhumane treatment of living beings.

CYBER THREATS:

- CYBER WAR (a term used to describe an activity aimed at gaining an advantage or superiority over an opponent in the management and use of communication and information channels or technologies),
- CYBER OCCUPATION OF THE COUNTRY (cyber-occupation is carried out by foreign powers
 through disinformation websites that make citizens unable to distinguish who is lying or
 telling the truth in the country, thus threatening the security, social, economic and legal
 stability of each country),
- CYBER-DISORIENTATION (due to disinformation websites, citizens are unable to distinguish between lies and the truth, which is a critically serious threat that can cause them death, health or financial harm),
- CYBER-TERRORISM (a premeditated politically motivated attack by organized groups, individuals or secret agents against information networks, computer programs and data, etc.),
- CYBER-ATTACKS (perpetrated by cyber criminals targeting strategic targets such as
 government offices, hospitals, NGOs and government institutions, classified information
 in the field of information and communication systems and cryptographic protection,
 etc.),
- CYBER-BULLYING (more than one third of the world's population faces cyber-bullying, which puts citizens at risk to life and limb),
- CYBER-TOTALITARIANISM (persecution of users of new technologies online, restriction of citizens' rights and freedoms in virtual space, etc.),
- CYBER-RACISM (social viruses that spread hatred through disinformation websites and social networks, giving birth to racism and terrorism),
- CYBER-LYNCH (occurs when people think serious abuse or injustice is being committed and a collective voice is created to seek justice; cyber-lynch often turns into destructive fanaticism),

- CYBER-HATE (because of the hatred that is mostly spread through disinformation websites
 and social networks, human lives and health are threatened, including the security, social,
 economic and legal stability of the country),
- CYBER-DICTATORSHIP (is one of the most feared global threats in the digital century, because of which the digital civilization faces psychological terror, injustice, discrimination, bullying, etc. from cyber-dictators, politicians, some public media that apply media manipulation, social networks, disinformation websites, cyber-terrorists and cyber-criminals),
- SOCIAL TERRORISM (is a form of brutal and insidious coercion by criminals and cyberthreat actors who attack strategic social targets and target sensitive areas where people are most vulnerable or completely defenseless and powerless),
- CYBER-CRIME (cyber-crime represents a significant part of overall crime, as evidenced by its share of total crime in the real world and in the virtual world).

The new global threats are irrefutable proof why reform of the international order is inevitable. The mission of the Action Plan - EU - 2023, which is presented to the EU member states and the European Commission by the international NGO Digital Policy Institute - millennium 3000 within the frame of the Cyber Summit on Fight against Disinformation - EU - 2023, is to prevent dictatorial regimes from occupying the European Union through disinformation websites and social networks.

Chapter 7

CYBER-POLICE - EU

The Cyber Summit on Fight against Disinformation - EU - 2023, presented to the EU member states by the international NGO Digital Policy Institute - millennium 3000, is also significant in another area, such as the announcement of the creation of a cyber police, not only at the European but also at the national level of the EU member states, without which the world in the digital age cannot do.

Cyber-police is a key body the mission of which is to protect digital society from threats and crimes committed in the virtual world that threaten human lives health, security, social, economic, energy, environmental and legal stability among people, nations and continents and principles of the rule of law.

The main reason why the Digital Policy Institute - millennium 3000 proposes the creation of the cyber politics is not only its indispensability in the digital age, but its immediate deployment, as most EU member states have established a cyber security authority to protect critical infrastructure, computers, mobile phones, etc., but politicians have completely forgotten to protect their citizens from threats and crimes committed in the virtual world, which include:

- social terrorism (threats and crimes committed in the virtual world),
- **social war** (the worst war in the history of mankind, waged by citizens against each other on social networks out of anger and hatred),
- **cyber-disinformation** (threatening not only human life and health, but also security, social, economic, energy, environmental and legal stability among people, nations and continents, and principles of the rule of law),
- social death (most often it appears wherever politicians go in the wrong direction and cannot resolve conflict situations, e.g. high inflation, collapsing political, social economic system, growing international tensions in the world, war conflicts, violence, lawlessness, racism, terrorism, the negative influence of disinformation websites that threaten the security, social, economic and legal stability of the country, the spread of hatred on social media that causes citizens to face personal, financial, health or mortal harm, COVID-19, corruption, etc.),
- **digital depression** (which is overwhelmingly affecting interpersonal relations, most often due to hate speech, spreading through disinformation websites and social networks faster than a coronavirus, and causing security and social tensions between people, nations and continents),
- **cyber-aggression** (it is much more dangerous than aggression itself, as social terrorists attack en masse, through social networks such as Facebook, TikTok, Instagram, Twitter, WhatsApp or Viber),

- cyber-lynching (it is an act of social terrorism in which perpetrators take the law into their own hands and spread misinformation on social media in order to stir up mass hatred against the person they are attacking),
- cyber-bullying (compared to traditional bullying, cyber-bullying is so destructive that it often
 drives citizens to commit suicide, preceded by a massive attack by social terrorists who use
 modern information and communication technologies, social networks, messengers or emails
 to commit social terrorism),
- **cyber-racism** (belongs to one of the most feared global threats of the millennium, as social terrorists spread it mainly through disinformation websites and social networks),
- **cyber-hate** (cyber-hate spread by social terrorists in the virtual world where the digital civilization, consisting of citizens of all nations, lives and works, has such a devastating effect that it can cause health or death to the victims),
- **cyber-defamation** (the goal of social terrorists is to damage the victim's reputation as much as possible or to completely disrupt the victim's life).

These threats and crimes committed in the virtual world are not the only reasons for the creation of cyber police and their immediate deployment.

Another reason for the creation of cyber police is that in the digital age, up to 80% of all threats and crimes will come from the virtual world.

The work of cyber-police will be different from its traditional work, but that does not change the fact that the following will depend on it:

- protection of life and health of citizens in both worlds (real and virtual) simultaneously,
- protection of human rights and freedoms in both worlds (real and virtual) simultaneously,
- ensuring security, social, economic and legal stability among people, nations and the continents,
- preventing the subversion of the political, social and legal systems in EU countries,
- preventing chaos and security, social and legal tensions between people, nations and continents,
- protecting the influence and dignity of the EU member states in global politics and international relations,
- protecting the national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- protecting the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- protecting a dignified position of the EU member states in the globally competitive environment,
- protecting the national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the

country and on which daily life depends, and includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),

- protecting the social capital (disrupted social relations lead to the destruction of the nation),
- protecting the cyber-economy on which the national and global economy existentially depends,
- protecting the digital identity of the citizen homo digitalis,
- environmental protection, including animals (includes all living and non-living things occurring in nature; it is a system composed of natural, artificial and social components of the material world that are or may be in constant interaction with the object under consideration).

Up to 70% of all cyber-police activity will be based on preventive measures that will contribute significantly to stopping the social war that citizens wage among themselves on social media because of anger and hatred, to establishing the digital peace on which global security and world peace depend, and to ending hostilities between people, nations and continents.

The establishment of digital peace and lasting security, social, economic, energy, ecological and legal stability among people, nations and continents depends 90% on prevention, which can be drawn from the material from which the international NGO Digital Policy Institute - millennium - 3000 plans to develop a methodological procedure to intervening against threats and crimes committed in the virtual world.

A set of modern preventive measures are parameters implemented to protect the digital society, the political, social and legal system and principles of the rule of law.

With respect to the increasing rate of cyber attacks by social terrorists, prevention is the most important tool of cyber police, as physical law enforcement means cannot be used against cyber threat actors in the virtual world.

The Digital Policy Institute - millennium 3000, an international NGO, will present to the European Commission and the EU member states the method and strategies for the implementation of preventive cyber police activities in the virtual world as part of the activation of the Action Plan - EU - 2023.

Chapter 8

CYBER-POLITICS - AN INTEGRAL PART OF THE NEW DIGITAL WORLD ORDER

The Cyber Summit on Fight against Disinformation - EU - 2023, presented to the EU member states by the international NGO Digital Policy Institute - millennium 3000, is a historic opportunity to officially embrace cyber-politics, which is already used for both worlds (real and virtual) simultaneously and has become an integral part of everyday life.

In the digital age, cyber-politics will serve to protect the digital society from social terrorism, which represents threats and crimes committed in the virtual world.

The word 'cyber-politics' is an unfamiliar concept for politicians, yet no politician in the world today can do without the term in his/her professional career.

Cyber-politics is most often carried out on social networks (Facebook, Instagram, Twitter, YouTube, TikTok, etc.) and has become an integral part of the new political scene, not only in the real but also in the virtual world in which the digital civilization, made up of citizens of all nations, lives.

Cyber-politics is irrefutable proof that the reform of the international order is no longer decided by politicians, but by the dynamic development of modern information and communication technologies and artificial intelligence, which is transforming traditional politics into cyber-politics and thus creating a new social and legal framework for the emergence of a new digital world order.

The digital century is a historical watershed between the past, present and future in which cyber politics will replace traditional politics, politicians and political parties, including backward political, legal and international systems.

The world has entered a digital age in which social networks are shaping the virtual form of interpersonal relationships, robotics are displacing human labour, computerization is changing the rules of the electoral system, artificial intelligence is contributing to the expansion of a new dimension of reality, offering new opportunities for innovative business and investment in nuclear, laser space, behavioral or blockchain technologies, nanotechnology, biotechnology, neural networks, telemedicine, circular, social and environmental economics, etc. And the dynamic development of modern information technology, which is behind the birth of cyber-politics, cannot be overlooked.

Current political party agendas are inapplicable to the digital age because they focus only on traditional issues (taxation, transport infrastructure, health, social policy, bureaucracy, etc.), but in the digital age it is essential to pay attention to new global threats, including threats and crimes committed in the virtual world.

The digital revolution is associated with a new global cultural diversity. The levelling of differences is due both to the natural blurring of cultural boundaries (politics, social culture, trade, advances in information and communication technologies with subsequent globalization) and to the direct

interest of states in increasing security, social, economic and legal stability and minimizing social conflict.

The new reality of the digital world is leading to the culmination of the process of mixing of peoples in the virtual world, while offering many opportunities to preserve social and cultural diversity, and, in addition, to engage in the digital, political, social, economic and legal process in their geographical area in order to preserve their social and national identity, traditions and beliefs.

Technological advances, especially in the dynamic development of modern information and communication technologies and artificial intelligence, bring entirely new concepts in the political, social, cultural and legal spheres that no country can do without in the future.

Reform of the international order is also inevitable for many other reasons, for example because threats and crimes have a corrosive effect on cyber-politics, of which the following is an integral part:

- digital civilization (digital civilization is made up of citizens of all nations),
- homo digitalis (digital personality),
- digitalization of politics (in the digital age, citizens will decide the future of their nation, through modern information and communication technologies),
- digitalization of power (all power will be transferred to modern information and communication technologies and artificial intelligence),
- cyber-politician (a cyber-politician is a person who uses modern information and communication technologies in his/her activities),
- digital sovereignty of the nation (the future of the nation in the digital age depends on digital sovereignty),
- digital identity of the nation and the citizen (without digital identity, the nation and the citizen would cease to exist),
- cyber-economy (national and global economies depend on cyber-economy),
- cyber-crime (cyber criminals use modern information and communication technologies as a tool to commit cyber crimes (e.g.: identity theft and theft of sensitive corporate information including personal data, cyber-vandalism, hacking, ransomware, cyber fraud, forgery, etc.) for ransom, extortion, etc., however, cyber-criminals are motivated only by profit generation, not by political or religious ideology or aspirations to carry out cyber attacks on a state and its people with the aim of overthrowing the government, threatening national security or principles of the rule of law),
- social terrorism (social terrorists are motivated by revenge, aggression, anger, resentment, power or economic interests, but also political ambitions, etc., and use modern information and communication technologies to create conflict situations and build a socially harmful environment in order to provoke social unrest in the country by spreading misinformation, chaos, fear, anger, distrust and hatred, thus endangering not only human life and health, but also national security and principles of the rule of law),
- cyber-terrorism (cyber-terrorists conduct ideologically (politically, religiously) motivated attacks against a state and its inhabitants (attacks on critical infrastructure, information

networks, computer programs, data, detection, disruption, encryption, destruction or sabotage of systems, attacks on energy, their storage, transport and production, attacks on drinking water production or distribution systems, attacks on the government sector, public administration, politics, attacks on banking systems, transportation, means of transport, attacks on traffic and air traffic control systems, hospitals, integrated rescue system units, military infrastructure, etc.)),

- cyber war (this is a term referring to activity aimed at gaining advantage or superiority over a rival in the control of modern information and communication technologies),
- cyber occupation (it is carried out by foreign powers through disinformation websites and social networks that make citizens no longer able to tell the lie from the truth, thus threatening the security, social, economic and legal stability of the country),
- cyber-defamation (a cyber-defamation is information that is untrue or highly distorted and the goal of perpetrators of social terrorism is to provoke hatred and hostility towards victims, damage their reputation and disrupt social relationships; cyber-defamation is one of the most widespread and feared global threats of the digital age, causing citizens around the world to face death, health, financial or personal harm),
- cyber-hate (the spread or promotion of cyber-hate threatens the security, social, economic and legal stability between people, nations and continents, and citizens face death, health, financial or personal harm because of it),
- cyber-racism (cyber-racism is the vilification of the human race, ethnic groups, national minorities, and citizens around the world face death, health, financial or personal harm because of it),
- cyber-bullying (cyber-bullying is harassment, verbal attacks, threatening the victim
 through modern information and communication technologies; online threats, aggressive
 or abusive texts, tweets, posts or messages, as well as posting personal data, pictures or
 videos to hurt or embarrass someone else are all included),
- cyber-perversion (cyber perverts pose a high security threat to society by producing,
 disseminating, sharing or promoting perverted, disgusting and life
 and health-threatening harmful content on the Internet, such as videos of crimes against
 humanity, cruel treatment of human beings or living beings, fulfill the elements of a
 particularly serious crime, support and promotion of social terrorism; cyber-criminals
 threaten the social health of society, on which the mental and physical health of human
 beings is existentially dependent),
- cyber-aggression (social terrorism can be defined as verbal assault, attack, insults, tantrums or threats that result in death, health, financial or personal harm to citizens),
- cyber-lynching (millions of citizens around the world are being pilloried on social media and humiliated and face death, health, financial or personal harm because of this brutal and insidious pressure),
- trolling (trolling is internet slang for situations that deliberately seek to stir up arguments,
 conflict and hostility in an online social community and use inflammatory messages to

- promote themselves in order to provoke emotional reactions and disrupt otherwise peaceful discussion),
- cyber-extremism (cyber-extremism is a particularly serious crime because it is characterized by the dissemination of political or ideological attitudes by which the perpetrators of social terrorism threaten not only an individual or a group, but above all the state, and in addition, they are attributed with violating rights and freedoms, including the basic principles of the constitutional order of the rule of law),
- cyber-dictatorship (is one of the most feared global threats in the digital century, because
 of which digital civilization faces psychological terror, injustice, discrimination, bullying,
 etc., by cyber-dictators, politicians, some public media that are using medial
 manipulation, social networks, disinformation websites, cyber-terrorists and cybercriminals; unlike the current dictatorship, cyber-dictatorship is much more dangerous,
 because whoever controls the virtual world through disinformation websites and social
 networks, controls the real world),
- cyber-discrimination (cyber-discrimination is a particularly serious crime involving unequal treatment, social injustice, threat to rights and freedoms, silencing, oppression, promotion and hatred of a different nationality, race and religion, obstruction or denial of the expression of a different opinion that is not contrary to the constitutional order of the rule of law, intimidation, threats, dehumanization of race and human dignity),
- fake accounts (setting up fake accounts to support and promote social terrorism or to commit cyber-crime is considered a particularly serious crime).

There are hundreds of new concepts and they will all become an integral part of our everyday lives.

Another key reason why it is necessary to reform the international order is that for the first time in history, citizens are living in two worlds (real and virtual) simultaneously, and this new dimension of reality requires a transformation of the political, social and legal system not only at the national level but also at the global level if global security is to be ensured.

In the cyber-future, it is necessary to ensure not only national but also global security, but these are not the same thing.

EU security encompasses everything related to the protection of Europe's infrastructure (national infrastructures are the interconnected devices, systems, information, people, networks and processes that are essential to the functioning of the global system and on which the daily lives of the virtual world and its people depend).

EU security involves the EU member states working together to ensure security, social, economic, energy, environmental and legal stability among people and nations.

In the cyber-future, national and global security can only be ensured if it is provided in both worlds (real and virtual) simultaneously; otherwise, the whole world risks facing global threats independently, exposing humanity to unspeakable cruelty.

The future of the European Union has a perspective if it includes new global and technological trends that will guarantee it complete security in both worlds (real and virtual) simultaneously and without which no EU member state can do without in the digital age.

Without digital integration, of which the fight against social terrorism is an integral part, the EU member states are at risk of the following:

- international isolation,
- digital isolation (threat to digital sovereignty, on which the fate of every nation depends),
- state disruption,
- threatening the security, social, economic and legal stability of the country,
- chaos,
- sharp rise in security and social tensions in the country,
- civil war,
- political, social and economic collapse,
- emigration,
- existential threat.

The task of the Action Plan - EU - 2023, which is presented to the EU member states and the European Commission by the international NGO Digital Policy Institute - millennium 3000 within the frame of the Cyber Summit on Fight against Disinformation - EU - 2023, is to build the digital integrity of the EU member states, without which the European Union would be at risk of disintegration.

Chapter 9

DWO

DIGITAL WORLD ORGANIZATION - THE NEW WORLD LEADER IN CYBER-FUTURE

WWW.DIGITALWORLDORGANIZATION.COM WWW.DIGITALNISVETOVAORGANIZACE.CZ

"No international organization on planet Earth is as organizationally prepared and technologically equipped for the cyber-future to protect the digital civilization made up of citizens of all nations as the new Digital World Organization."

The United Nations has certainly done a lot of good in its 78 years of existence, but it is beyond its capacity to combat new global threats and crimes committed mainly in the virtual world. The year 2023 is a historic opportunity for the creation of the Digital World Organization (DWO), the key mission of which will be:

- to carry out peaceful activities in the virtual world on which global security, world peace and the protection of human rights and freedoms depend,
- to protect the digital civilization, made up of citizens of all nations, from threats and crimes committed in the virtual world,
- to stop the social war that citizens wage among themselves because of anger and hatred,
- to establish the digital peace on which global security depends, and world peace and the protection of human rights and freedoms.

In 1945, no one in the world could have guessed that in the year 2000, a new virtual world would be born into which an entire civilization would move, one day needing protection from cyber-criminals and social terrorists who create conflict situations and build socially harmful environments in cyber-space with the aim of creating social unrest in the country primarily by spreading misinformation, chaos, fear, anger, distrust and hatred.

Today, people live in both worlds (real and virtual) simultaneously, and it is therefore more necessary than ever to ensure the protection of the digital civilization, which is made up of citizens of all nations.

In the digital century, the real world is becoming existentially dependent on the virtual world not only for global security but also for the cyber-economy, which will account for up to 70% of global GDP in the cyber-future.

Today, there is little doubt that the fate of the entire world in the digital age depends on digital peace.

The Digital World Organization (DWO) will be obliged to:

- to carry out peaceful activities in the virtual world,
- to build digital peace on which global security and world peace depend,
- to protect the digital civilization, which consists of citizens of all nations, from cyber threats and crimes committed in the virtual world,
- to protect innocent victims from the social war that people wage against each other on social media because of anger and hatred,
- to protect human rights and civil freedoms in the virtual world,
- to protect the lives and health of citizens in the virtual world,
- to protect the national and digital sovereignty of the DWO member states in the virtual world (digital sovereignty means the ability to control one's destiny in the real world, and data, hardware and software in the virtual world),
- to protect the national and digital identity of the DWO member states in the virtual world (a nation's digital identity is crucial to its influential and dignified position not only in the real world but also in the virtual world),
- to protect the cyber-economy of the DWO member states in a virtual world on which the national and global economy is existentially dependent,
- to protect thenational principles of the DWO member states in the virtual world (national principles set out a nationally consistent approach to the creation of social and cultural values protection of human rights and freedoms, lasting security, social, economic and legal stability in the country, protection of the environment, care for animals, etc.),
- to preserve the national, social and cultural history of the DWO member states in the virtual world (history, traditions, customs and customs, communities, language, social, legal and spiritual culture, personalities and authorities of the nation, ideas, opinions, values and attitudes, visions and ideas, sovereignty of the nation, self-confidence of the nation, unrestricted will to decide its own identity and future, ability and determination to defend national identity and national dignity, etc.),
- to protect the national assets of the DWO member states in the virtual world (language, national sovereignty, social and cultural history, traditions, customs, customs, ethical, moral and social norms, social identity, national identity, national virtues, dignity of the nation, social, financial and spiritual capital, environment, animals, ecosystem, etc.),
- to protect the environment through modern technologies and ensure environmental peace (environment and peace are key in all areas of conservation, sustainable development and security, with a focus on integrating nature conservation and prevention of environmental conflicts and disasters, including animal protection).

THERE IS A PROMISING HOPE that, for the first time in history, it will be the European Union that, already in its role as a digital leader, will welcome the new member states of the Digital World Organization to the European continent.

THERE IS A PROMISING HOPE that, for the first time in history, it will be the European Union, already in its role as a digital leader, that will cut the ribbon on the new Digital World Organization building, to which it will introduce the new DWO member states.

THERE IS A PROMISING HOPE that, for the first time in history, it will be the European Union, already in its role as a digital leader, that will provide the new member states of the Digital World Organization with the diplomatic background on the European continent to carry out their mission for the digital civilization made up of citizens of all nations.

The DWO member states' costs on the creation of the Digital World Organization is the best investment in cyber-future, because the fate of the entire world depends on digital peace.

In a virtual world where there are no national borders, today more than 6 billion users of modern information and communication technologies live together as one big community, regardless of race, nationality, language, color, political or sexual orientation or religion, and this new community is called digital civilization.

The future of the entire world depends on digital peace, and therefore the task of the Digital World Organization is to protect the DWO member states from cyber threats and crimes committed in the virtual world that:

- threaten the lives and health of citizens,
- disrupt the security, social, economic and legal stability between people, nations and continents,
- subverts the political, social and legal system in every country,
- cause chaos and security, social and legal tensions between people, nations and continents,
- undermine the influential and dignified position of the state in global politics and international relations,
- distort a country's national and digital sovereignty in the virtual world (cyber-space),
- challenge the influential and dignified position of states in the global competitive environment,
- destabilize the national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and also includes some functions, locations and organizations that are not critical to the maintenance of essential services but that need protection because of the potential danger to the public),

- damage social capital (disrupted social relations lead to the destruction of the nation),
- cripple the cyber-economy on which the national and global economy is existentially dependent,
- damage the digital identity of the citizen homo digitalis,
- denigrate the digital sovereignty of the nation, which no country can do without in the digital age,
- devastate the environment and abuse animals (includes all living and non-living things found in nature; it is a system composed of natural, artificial and social components of the material world that are or may be in constant interaction with the object under consideration).

The creation of a new Digital World Organization is inevitable because someone has to protect digital civilization, or rather the more than 6 billion users of modern information and communication technologies who live together in the virtual world as one big community, regardless of race, nationality, language, color, political or sexual orientation or religion.

THERE IS A PROMISING HOPE that, for the first time in history, it will be the European Union that, already in its role as a digital leader, will announce the creation of a new Digital World Organization at the Cyber Summit on Fight against Disinformation - EU - 2023.

THERE IS A PROMISING HOPE that, for the first time in history, it will be the European Union, which, already in its role of digital leader, will announce at the Cyber Summit on Fight against Disinformation - EU - 2023 that the building of the new Digital World Organization will symbolically stand in the EU member state in Prague, where the idea (of its founder Ladislav Boldi) was first born.

THERE IS A PROMISING HOPE that, for the first time in history, it will be the European Union, already in its role as a digital leader, that will announce at the Cyber Summit on Fight against Disinformation - EU - 2023 that the Digital World Organization will launch its activities by the end of 2023 at the latest, in order to accelerate the protection of the digital civilization, which is currently facing cyber threats that are spilling over into the real world and threatening global security, human rights and freedoms and world peace.

THERE IS A PROMISING HOPE that, for the first time in history, it will be the European Union that will welcome not only the United States of America, but also a number of no less important new DWO member states in the role of digital leader by the end of 2023 at the latest in the new Digital World Organization building.

The Digital World Organization is the only international organization in the world that is organizationally and technologically top-equipped to ensure that the digital civilization, which

consists of citizens of all nations, is protected from threats and crimes committed in the virtual world, including:

SOCIAL WAR (which citizens wage among themselves on social networks because of anger and hatred),

SOCIAL TERRORISM (threats and crimes committed in the virtual world),

CYBER MURDER (a cyber-murderer is a person or legal entity that spreads rumors, hate, racism, terrorism, bullying, aggression, lynching, extremism, or misinformation that causes citizens to take their own lives. This is a completed crime of cyber murder),

CYBER-DEFAMATION (a cyber-defamation is information that is untrue or significantly distorted, and the goal of perpetrators of social terrorism is to provoke hatred and hostility towards victims, damage their reputation, and disrupt social relationships; cyber-defamation is one of the most prevalent and feared global threats of the digital century, causing citizens around the world to face death, health, financial, or personal harm),

CYBER-HATE (the spread or promotion of cyber-hate threatens the security, social, economic and legal stability between people, nations and continents and citizens face death, health, financial or personal harm because of it),

CYBER-RACISM (is the vilification of the human race, ethnic groups, national minorities, and citizens around the world face death, health, financial or personal harm because of it),

CYBER-BULLYING (is harassment, verbal attacks, threatening the victim, through modern information and communication technologies; online threats, aggressive or abusive texts, tweets, posts or messages, as well as posting personal data, pictures or videos intended to hurt or embarrass someone else are included),

CYBER-PERVERSION (cyber perverts pose a high security threat to society by producing, distributing, sharing or promoting perverse, disgusting and harmful content on the Internet that endangers life and health, such as videos of crimes against humanity, cruelty to human beings or to living beings, thus fulfilling the elements of the particularly serious crime of supporting and promoting social terrorism; cyber-perverts threaten the social health of society, on which the mental and physical health of the individual is existentially dependent),

CYBER-AGGRESSION (social terrorism can be defined as verbal assault, attack, insults, tantrums or threats that result in death, health, financial or personal harm to citizens),

CYBER-LYNCHING (millions of citizens around the world are pilloried and humiliated on social networks and face death, health, financial or personal harm because of this brutal and insidious pressure),

TROLLING (is internet slang for situations that deliberately seek to stir up arguments, conflict and hostility in an online social community and use inflammatory messages to promote themselves in order to provoke emotional reactions and disrupt otherwise peaceful discussion),

CYBER-EXTREMISM (is a particularly serious crime, as it is characterized by the dissemination of political or ideological attitudes, which the perpetrators of social terrorism use to threaten not only an individual or a group, but above all the state, and in addition, they are also attributed with

violating rights and freedoms, including the basic principles of the constitutional order of the rule of law),

CYBER-DISINFORMATION (is false or unverified information (lies, fake news, manipulation of public opinion, alarmist messages, propaganda, etc.) that causes citizens to face mortal, health, financial or personal harm because they are unable to distinguish lies from the truth in time), **CYBER-DICTATORSHIP** (is one of the most feared global threats in the digital century, because of which the digital civilization faces psychological terror, injustice, discrimination, bullying, etc. from cyber-dictators, politicians, some public media that apply media manipulation, social networks, disinformation websites, cyber-terrorists and cyber-criminals; unlike the current dictatorship, cyber-dictatorship is much more dangerous, because whoever controls the virtual world through disinformation websites and social networks, the one controls the real world),

CYBER-DISCRIMINATION (is a particularly serious crime involving unequal treatment, social injustice, threat to rights and freedoms, silencing, oppression, support and promotion of hatred against a different nationality, race and religion, obstruction or denial of the expression of a different opinion that is not contrary to the constitutional order of the rule of law, intimidation, threats, dehumanization of race and human dignity),

CYBER-PARAPHILIA (social terrorism can be defined as the criminal behavior of a paraphiliac who, because of his/her sexual disorder, endangers the lives and health of citizens or their safety and privacy),

FAKE ACCOUNTS (setting up fake accounts to support and promote social terrorism or to commit cyber-crime is considered a particularly serious crime),

CYBER-CANNIBALISM (cyber cannibals scour the web-blogs, forums, anywhere personal information about the victim can be found - and peer into the deepest recesses of life, literally devouring people's privacy, exposing all secrets and engaging in targeted attacks in search of the human body),

CYBER WAR (a term used to describe an activity aimed at gaining an advantage or superiority over an opponent in the management and use of communication and information channels or technologies),

CYBER OCCUPATION OF THE COUNTRY (cyber-occupation is carried out by foreign powers through disinformation websites that make citizens unable to distinguish who is lying or telling the truth in the country, thus threatening the security, social, economic and legal stability of every country),

CYBER-TERRORISM (a premeditated politically motivated attack by organized groups, individuals or secret agents against information networks, computer programs and data, etc.),

CYBER-DISORIENTATION (due to the spread of misinformation, citizens are unable to distinguish between lies and truth; cyber-disorientation causes death, health or financial harm to citizens),

CYBER-ATTACKS (perpetrated by cyber criminals and targeting strategic targets such as government offices, hospitals, NGOs and government institutions, classified information in the field of information and communication systems and cryptographic protection, etc.),

CYBER-TOTALITARIANISM (persecution of users of new technologies online, restriction of citizens' rights and freedoms in virtual space, etc.),

CYBER-CRIME (general crime is the most significant part of the total crime, as evidenced by its share in the total crime in the real world and in the virtual world; general crime includes both violent and non-violent forms of crime, which, due to their social danger, significantly influence the public opinion of citizens about their safety).

IMPORTANT INFORMATION

The Cyber Summit on Fight against Disinformation - EU - 2023 will be the official venue where the Digital Policy Institute - millennium 3000 will hand over to the European Commission all the documents and documents related to the creation of the Digital World Organization (DWO), the registration of which was made in the EU member state, in Prague, under the file number: **L101F**.

WARNING

Because of the increasing threats and crimes committed in the virtual world, which are massively migrating to the real world faster than COVID-19, it is essential that the Digital World Organization launches its activities to protect the digital civilization, which consists of citizens of all nations, no later than the end of 2023.

The organizational structure of the Digital World Organization is also available on the website www.digitalworldorganization.com.

Chapter 10

THE DIGITAL WORLD ORGANIZATION AND THE NEW DIGITAL WORLD ORDER

In the digital century, the fate of humanity will depend on the Digital World Organization (DWO), as 80% of global threats come from the virtual world where social war and social terrorism rage, and no government in the world has the means to prevent these threats in their own country. The Digital World Organization (DWO), as the world's only one, has modern, technologically advanced tools and a set of advanced preventive measures to defeat the social terrorism worldwide that the following is currently put at risk:

- digital peace,
- global security,
- world peace,
- lives and health of citizens in both worlds (real and virtual) simultaneously,
- rights and freedoms in both worlds (real and virtual) simultaneously,
- security, social, economic and legal stability among people, nations and continents,
- an influential and dignified position of the EU member states in global politics and international relations,
- national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- a dignified position for the EU member states in a globally competitive environment,
- national Infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and also includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- social capital (disrupted social relations lead to the destruction of the nation),
- cyber-economy, on which the national and global economy is existentially dependent,
- digital identity of the citizen homo digitalis,
- environment, including animals (includes all living and non-living things occurring in nature; it is a system composed of natural, artificial and social components of the material world that are or may be in constant interaction with the object under consideration).

No government in the world is capable of defending itself against social terrorists because it lacks the modern, technologically advanced tools and advanced set of preventive measures that only the Digital World Organization has.

Thanks to new technological tools and a modern set of preventive measures, the Digital World Organization (DWO) is able to ensure the protection of member states from social terrorists who are willing and ready because of power or economic interests, anger, hatred, etc.:

- to unleash the subversion of the nation,
- to provoke political, social, economic and legal collapse,
- to threaten the security, social, economic and legal stability of the country,
- to cause security and social tensions in society,
- to destabilize the national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and also includes some functions, locations and organizations that are not critical to the maintenance of essential services but that need protection because of the potential danger to the public),
- to cripple the cyber-economy on which the national and global economy is existentially dependent,
- to damage social capital (disrupted social relations lead to the destruction of the nation),
- to provoke massive protests and demonstrations against the government, ministries, state authorities and public administration, etc.

When citizens (children and adults, individuals or corporations, politicians, governments, etc.) create a harmful social (conflict) environment around them, whether in the real or virtual world (cyber-space), that causes their fellow citizens to face personal, financial, health, or mortal harm, they become social terrorists.

The most common reasons why citizens (children, adults, individuals or corporations, politicians, governments, etc.) become social terrorists include frustration, anger, hatred, disappointment, failure, despair, personal strife, social isolation, loneliness, poverty, hopelessness, social, religious, sexual or political disorientation, insults, humiliation, power or economic interests, corruption, etc. The goal of social terrorists is to gain visibility, harm, revenge, harm, intimidate, prey on, threaten, or control an individual, group, or state (even a foreign state) for the purpose of power or economic interests.

For the first time in human history, citizens are living in two worlds (real and virtual) simultaneously, but they no longer feel safe in either.

Smartphones, mobile internet, social networks such as Facebook, TikTok, Instagram, Twitter, WhatsApp or Viber are nowadays one of the key tools for perpetrating social terrorism that moves from the virtual world to the real one.

The mission of the Digital World Organization, which has modern, technologically advanced tools and a set of modern preventive measures to combat social terrorism, will reliably ensure the

protection of member states (DWO) from social terrorists who use the following to commit crimes against humanity:

- modern information and communication technologies,
- disinformation websites,
- social networks (Facebook, TikTok, Instagram, Twitter, WhatsApp or Viber, etc.)

No government in the world is able to defeat social terrorism, or stop social warfare, establish digital peace, or stop social terrorists from abroad on its own because it lacks the modern, technologically advanced tools and advanced set of preventive measures that only the Digital World Organization has.

As a result of social terrorism and the social war that citizens wage among themselves on social media, due to anger and hatred, there is a sharp increase of the conflict situations in every country from which the following is born:

- chaos,
- disorientation,
- frustration,
- anger,
- fear,
- panic anxiety,
- vindictiveness,
- distrust,
- despair,
- hopelessness,
- disappointment,
- irritability,
- hatred.

WARNING

Because of the increasing threats and crimes being committed in the virtual world, which are massively migrating to the real world faster than COVID-19, it is essential that the Digital World Organization launches its activities to protect the digital civilization, which consists of citizens of all nations, no later than the end of 2023.

The organizational structure of the Digital World Organization is also available on the website www.digitalworldorganization.com.

Chapter 11

DIGITAL WORLD ORGANIZATION - BUILDER OF DIGITAL PEACE AND PROTECTOR OF DIGITAL CIVILIZATION

Quotation:

"The future of humankind depends on digital peace in the virtual world."

The only way to prevent threats and crimes committed in the virtual world from having a corrosive impact on the real world is for the Digital World Organization to build digital peace, in addition to protecting the digital civilization made up of citizens of all nations, because the following depends on digital peace:

- protection of life and health of citizens in both worlds (real and virtual) simultaneously,
- protection of human rights and freedoms in both worlds (real and virtual) simultaneously,
- ensuring security, social, economic and legal stability among people, nations and the continents,
- preventing the subversion of the political, social and legal systems in EU countries,
- preventing chaos and security, social and legal tensions between people, nations and continents,
- protecting the influence and dignity of the EU member states in global politics and international relations,
- protecting the national and digital sovereignty and identity of the EU member states in both worlds (real and virtual) simultaneously,
- protecting the social and cultural history of the EU member states in both worlds (real and virtual) simultaneously,
- protecting a dignified position of the EU member states in the globally competitive environment,
- protecting the national infrastructure (national infrastructure is the facilities, systems, locations, information, people, networks and processes that are essential to the functioning of the country and on which daily life depends, and includes some functions, locations and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- protecting the social capital (disrupted social relations lead to the destruction of the nation),
- protecting the cyber-economy on which the national and global economy existentially depends,
- protecting the digital identity of the citizen homo digitalis,

environmental protection, including animals (includes all living and non-living things occurring
in nature; it is a system composed of natural, artificial and social components of the material
world that are or may be in constant interaction with the object under consideration).

The Digital World Organization will promote a peace policy based not on protection but on building digital peace.

In order to prevent war from ever happening again, peace cannot be made, negotiated or protected, as politicians and many others (diplomats, advisors, philosophers, historians, scholars, scientists, teachers, etc.) have mistakenly believed for millennia; peace must only be built. It is a somewhat curious fact that in the history of mankind there has not been a great man (wise man, politician, diplomat, counselor, philosopher, historian, researcher, scientist, teacher or journalist) who has paid attention to mapping the peace structure that constitutes the principles of peace.

It is a somewhat curious fact that in the history of mankind there has not been a great man (wise man, politician, diplomat, advisor, philosopher, historian, researcher, scientist, teacher or journalist) who has enriched mankind with the most important thing on which the fate of the whole world depends, which is the mapping of the peace structure and explaining the following to mankind:

- what peace is between people, nations and continents (where there is anger and hatred, there can be no peace),
- out of which peace is born and created,
- what makes up the tribal structure of peace,
- on what all peace depends,
- what makes up the hierarchy of the peace system,
- how peace is made,
- who can make peace,
- what is the personal, moral, social, spiritual and financial value of peace,
- how peace is integrated into the formation of social integrity,
- by what means peace is maintained,
- by what means peace is secured,
- what digital peace is and why the fate of the world depends on it,
- out of which digital peace is born,
- what makes up the tribal structure of digital peace,
- on what all digital peace depends,
- what makes up the hierarchy of the digital peace system,
- how digital peace is made,
- who can make digital peace,

- what is the personal, moral, social, spiritual and financial value of digital peace,
- how peace is being integrated into the formation of the digital society,
- by what means digital peace is maintained,
- by what means digital peace is secured.

Everyone talks or writes about peace, but no one in the world knows the principles of peace as well as the Digital World Organization does.

Peace is not to be made, negotiated or protected; peace must be built so that war can never happen again.

If someone wants to negotiate, make or protect peace, he is acting in contradiction to the Principles of Peace, because peace is not to be made, negotiated or protected, peace must be built, otherwise there is again the threat of war.

That peace is not to be made, negotiated, protected, but built, is a revolutionary idea based on many-years empirical research by Ladislav Boldi, author of the book Cyber Summit on Fight against Disinformation - EU - 2023, who has investigated why wars recur even though peace has been made or negotiated.

A landmark event in human history, the 'Principles of Peace' will become the cornerstone of digital peace, on which global security, world peace and the protection of human rights and freedoms depend.

If politicians find themselves in a situation where they claim they have to protect the peace, this is indisputable proof that they have built peace badly, or not at all.

Therefore, the Digital World Organization will promote a peace policy based not on protection but on building digital peace.

For the first time in history, citizens are living in two worlds (real and virtual) simultaneously, as one large community, regardless of nationality, political ideology or religion, and this new combined environment that has been created on planet Earth represents a whole new dimension of reality for the digital century in which humanity finds itself.

In this new dimension of reality, which is called metaverse, a networked online space with a digitally persistent environment is created, which people inhabit already as homo digitalis. For citizens, the virtual world has become a second home in which they live and work, and for this reason it is necessary to establish law and order in cyber-space, or to build a new digital political, social and legal infrastructure to ensure the protection of life, health and rights of homo digitalis. However, in addition to the digital political, social and legal infrastructure, a new digital administrative and governance system for public, social and health services, digital security bodies to maintain order within cyber-space, a new digital education system, etc. will also need to be built in the virtual world.

In the virtual world that has become a second home for humanity, the Digital World Organization (DWO) will represent the needs and interests of the digital civilization made up of citizens of all nations.

In order to establish law and order in the virtual world, the Digital World Organization (DWO) must launch its activities as soon as possible, which, in addition to building a new digital political, social and legal infrastructure, including digital amenities for public, social and health services, will also cover new digital administrative and governance systems, security bodies designed to maintain order within the online environment, a new digital education system for homo digitalis, etc.

Law and order must be respected by all citizens, because in the virtual world more than 6 billion citizens - homo digitalis - live together as one big community, without borders and regardless of race, nationality, language, color of skin, political ideology or religion.

THREAT TO DIGITAL PEACE

Quotation:

"The world is ceasing to function, states are not prepared to solve problems."

António Guterres, the UN Secretary-General

UN Secretary-General António Guterres unwittingly initiated the creation of a new Digital World Organization with his quote, because real-world peace and lasting security, social, economic, energy, environmental and legal stability among people, nations and continents depend on digital peace in the virtual world.

To ensure the protection of citizens and national security, the EU member states need to adopt the Law on Combating Social Terrorism, and if they do so, this will be a historic event in the digital century, as crimes committed in the virtual world (brutal attacks by social terrorists, spreading misinformation, anger, revenge, incitement to hatred, etc.) threaten up to 80% of the real world, in which conflict situations between people, nations and continents arise.

If the EU member states do not make a concerted effort to accelerate the emergence of the Digital World Organization, the following will be at immediate risk:

- the security, social, economic, energy, environmental and legal stability of the EU,
- principles of the rule of law in the EU member countries,
- the national security of the EU member countries,
- the activities of officials in the EU member countries,
- social stability in the EU member countries,
- the national economies of the EU member countries,
- digital sovereignty of the EU member countries,

- interpersonal, virtual and international relations between the EU member countries,
- Europe's infrastructure (facilities, systems, places, information, people, networks and processes that are essential to the functioning of a country and on which everyday life depends).

Politicians and state authorities themselves probably had no idea of the destructive power of social terrorism, which threatens the digital civilization made up of citizens of all nations.

Goals of the Digital World Organization (DWO):

- to build digital peace,
- to protect the digital civilization made up of citizens of all nations,
- to protect the lives and health (social, mental and physical) of citizens in the virtual world,
- to ensure security, social, economic and legal stability in the virtual world,
- to protect human rights and freedoms in the virtual world,
- to protect the digital sovereignty of the DWO member states in the virtual world,
- to protect the digital identity of the DWO member states in the virtual world (preserving the social and cultural history of nations),
- to protect the social, economic and legal integrity of the DWO member states in the virtual world,
- to protect social capital (interpersonal, virtual and international relationships),
- to protect digital infrastructure (digital infrastructure is the equipment, systems, places, information, people, networks and processes that are essential to the functioning of the country and on which everyday life depends, and also includes some functions, places and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- to protect animals (animal cruelty is an act of social terrorism, as animals are an integral part of modern civilization, not only in personal or professional life, but also in public life).

Visions of the Digital World Organization (DWO):

Among the key visions of the Digital World Organization is the sharing of generally universal values and rules to enable:

- to build digital peace in the virtual world so that GLOBAL (security, social, health, economic, environmental and cyber) THREATS can no longer be transmitted to the real world,
- to build a new global political system with a modern social and legal infrastructure designed for the new millennium, linking the real world with the virtual world in which the digital civilization made up of citizens of all nations lives,
- to build a new digital agency, the Cyber Police, with its representation in each DWO
 member state, to ensure the security of citizens homo digitalis, maintain public order,
 enforce the digital law and detect and investigate crime, including particularly serious
 crimes such as social terrorism and social war in the virtual world,

- to build a digital rapid reaction force, which will be represented in each DWO member state and its mission will be to ensure the security of citizens - homo digitalis in a virtual world that needs to be protected from social terrorists (digital special commandos, digital rapid reaction units, digital security forces, digital operational raid squads, digital protection service, etc.),
- to build a new digital health organization, with a presence in each DWO member state, the mission of which will be to ensure the protection of healthy citizens homo digitalis in a virtual world, as the right to health is considered one of the most fundamental rights of every human being under the digital law, regardless of race, religion, political beliefs, economic or social status,
- to build a digital world bank that will work to reduce poverty, help socially and medically
 disadvantaged citizens as well as individuals and corporations by promoting and
 developing the cyber economy (on which the national and global economy depends), and
 support developing countries and economies in transition; digital loans and digital deposits
 can be used to achieve these goals,
- a digital trade organization, the mission of which will be to promote the cyber economy, implement digital rules in the operation of digital trade, provide digital assistance to developing countries, collaborate with other international organizations, etc.,
- to build a digital prosecutor's office (a digital prosecutor is a person who is commissioned by the Digital World Organization to represent the interests of the DWO member states in criminal proceedings when cyber crimes are committed that threaten the digital civilization, which consists of citizens of all nations, social terrorism, social wars, etc.),
- **to build a digital court** to adjudicate on actions brought by the state authorities (powers) of the DWO member states.

WARNING

Because of the increasing threats and crimes being committed in the virtual world, which are massively migrating to the real world faster than COVID-19, it is essential that the Digital World Organization launches its activities to protect the digital civilization, which consists of citizens of all nations, no later than the end of 2023.

The organizational structure of the Digital World Organization is also available on the website www.digitalworldorganization.com.



Chapter 12

ORGANIZATIONAL STRUCTURE OF THE DIGITAL WORLD ORGANIZATION

PRESIDENT OF DWO

The Digital World Organization (DWO) is represented by the President, whose mission is to represent the digital civilization, which is made up of citizens of all nations, and to consistently protect their interests, needs and rights.

The President of the Digital World Organization is elected by the DWO Digital Assembly for a fiveyear term through electronic elections.

Citizens (homo digitalis) of all nations live together in the virtual world, as one large community, regardless of nationality, political ideology or religion, and therefore the legal duty of the President of the Digital World Organization is:

- to protect digital peace in the virtual world,
- to protect the digital civilization made up of citizens of all nations,
- to protect the lives and health (social, mental and physical) of citizens in the virtual world,
- to ensure security, social, economic and legal stability in the virtual world,
- to protect human rights and freedoms in the virtual world,
- to protect the digital sovereignty of the DWO member states in the virtual world,
- to protect the digital identity of the DWO member states in the virtual world (preserving the social and cultural history of nations),
- to protect the social, economic and legal integrity of the DWO member states in the virtual world,
- to protect social capital (interpersonal, virtual and international relationships),
- to protect digital infrastructure (digital infrastructure is the equipment, systems, places, information, people, networks and processes that are essential to the functioning of the country and on which everyday life depends, and also includes some functions, places and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- to protect animals (animal cruelty is an act of social terrorism, as animals are an integral part of modern civilization, not only in personal or professional life, but also in public life).

The President of the DWO may never act contrary to the principles of the Digital World Organization the mission of which is as follows:

- protecting the virtual world from GLOBAL (security, social, health, economic, environmental and cyber) THREATS,
- protecting the digital civilization made up of citizens of all nations,
- protecting the digital law, which will be legally binding for the DWO member states, the digital law is a set of generally binding rules of conduct of the digital civilization in the virtual world,
- protecting the digital charter of rights and freedoms, which will be legally binding on the DWO member states,
- protecting the digital sovereignty of the DWO member states,
- protecting the digital identity of the citizen homo digitalis,
- protecting the cyber economy on which the national economies of the Digital World
 Organization member states existentially depend,
- animal protection (animal cruelty is an act of social terrorism, as animals are an integral part of modern civilization, not only in personal or professional life, but also in public life).

The President of the DWO has a staff of international officials who are responsible only to him and not to governments.

The President of the DWO signs the digital laws submitted to him for approval by the Digital Security Council - DWO, or must veto them if they conflict with the principles of the Digital World Organization.

Without the signature of the President of the DWO, the digital laws are null and void and therefore may not be applied.

Should the DWO President act contrary to the principles of the Digital World Organization, then it is the legal duty of the DWO Digital Assembly to call a vote for immediate removal from office.

Should the DWO President act contrary to the principles of the Digital World Organization, a supermajority vote of the Digital Assembly is required to remove him from office immediately.

DIGITAL ASSEMBLY

The Digital World Organization (DWO) is represented by the Digital Assembly, made up of the DWO member states, the mission of which is to represent the digital civilization made up of citizens of all nations and to consistently protect its interests, needs and rights.

The Digital Assembly meets regularly every month, more frequently only according to urgency and need.

The DWO member states meet in different configurations, each corresponding to a specific political area to be discussed. Depending on the composition, each country sends the member of the government responsible for that area to the Assembly.

Citizens (homo digitalis) of all nations live together in the virtual world, as one big community, regardless of nationality, political ideology or religion, and therefore the legal obligation of the Digital Assembly will be jointly:

- to protect digital peace in the virtual world,
- to protect the digital civilization made up of citizens of all nations,
- to protect the lives and health (social, mental and physical) of citizens in the virtual world,
- to ensure security, social, economic and legal stability in the virtual world,
- to protect human rights and freedoms in the virtual world,
- to protect the digital sovereignty of the DWO member states in the virtual world,
- to protect the digital identity of the DWO member states in the virtual world (preserving the social and cultural history of nations),
- to protect the social, economic and legal integrity of the DWO member states in the virtual world.
- to protect social capital (interpersonal, virtual and international relationships),
- to protect digital infrastructure (digital infrastructure is the equipment, systems, places, information, people, networks and processes that are essential to the functioning of the country and on which everyday life depends, and also includes some functions, places and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- to protect animals (animal cruelty is an act of social terrorism, as animals are an integral part of modern civilization, not only in personal or professional life, but also in public life).

No member state of the Digital Assembly may ever act contrary to the principles of the Digital World Organization, the mission of which is:

- protecting the virtual world from GLOBAL (security, social, health, economic, environmental and cyber) THREATS,
- protecting the digital civilization made up of citizens of all nations,
- protecting the digital law, which will be legally binding for the DWO member states, the digital law is a set of generally binding rules of conduct of the digital civilization in the virtual world,
- protecting the digital charter of rights and freedoms, which will be legally binding on the DWO member states,
- protecting the digital sovereignty of the DWO member states,
- protecting the digital identity of the citizen homo digitalis,
- protecting the cyber economy on which the national economies of the Digital World
 Organization member states existentially depend,

• animal protection (animal cruelty is an act of social terrorism, as animals are an integral part of modern civilization, not only in personal or professional life, but also in public life).

Each DWO member state has a staff of international officials who are responsible only to it and not to governments.

The DWO member states will approve the digital laws on the ground of the Digital Assembly submitted to them for approval by the Digital Security Council - DWO, but they can only approve them on condition that they do not contradict the principles of the Digital World Organization. Without the approval process, the digital laws submitted to the Digital Assembly for approval by the Digital Security Council - DWO will be invalid and may not be applied.

The DWO member states have the right to propose the digital laws of their own volition and the Digital Security Council - DWO is obliged to consider and receive them for processing, as long as they do not conflict with the principles of the Digital World Organization.

Should any member state of the DWO act in contradiction to the principles of the Digital World Organization, then it is the legal duty of the Digital Assembly to call a vote to expel it from the Digital World Organization immediately.

Should any DWO member state act contrary to the principles of the Digital World Organization, a supermajority in the Digital Assembly is required for its immediate expulsion from the Digital World Organization.

DIGITAL SECURITY COUNCIL - DWO

The Digital Security Council - DWO is made up of 21 members whose mission is to represent the digital civilization, which consists of citizens of all nations, and to consistently protect its interests, needs and rights.

Members of the Digital Security Council - DWO are elected by the Digital Assembly for a five-year term through electronic elections.

The Digital Security Council - DWO will meet regularly once a month and will convene the Digital Assembly according to urgency and need.

The members of the Digital Security Council - DWO rotate the chairmanship every three months. The mission of the Digital Security Council - DWO is to develop proposals for the digital laws to be submitted to the Digital Assembly for approval, in order to:

- protecting the virtual world from GLOBAL (security, social, health, economic, environmental and cyber) THREATS,
- protecting the digital civilization made up of citizens of all nations,
- protecting the digital law, which will be legally binding for the DWO member states, the
 digital law is a set of generally binding rules of conduct of the digital civilization in the
 virtual world,
- protecting the digital charter of rights and freedoms, which will be legally binding on the DWO member states,

- protecting the digital sovereignty of the DWO member states,
- protecting the digital identity of the citizen homo digitalis,
- protecting the cyber economy on which the national economies of the Digital World Organization member states existentially depend,
- animal protection (animal cruelty is an act of social terrorism, as animals are an integral part of modern civilization, not only in personal or professional life, but also in public life).

Citizens (homo digitalis) of all nations live together in the virtual world, as one big community, regardless of nationality, political ideology or religion, and therefore the legal obligation of the Digital Security Council - DWO shall be:

- to protect digital peace in the virtual world,
- to protect the digital civilization made up of citizens of all nations,
- to protect the lives and health (social, mental and physical) of citizens in the virtual world,
- to ensure security, social, economic and legal stability in the virtual world,
- to protect human rights and freedoms in the virtual world,
- to protect the digital sovereignty of the DWO member states in the virtual world,
- to protect the digital identity of the DWO member states in the virtual world (preserving the social and cultural history of nations),
- to protect the social, economic and legal integrity of the DWO member states in the virtual world,
- to protect social capital (interpersonal, virtual and international relationships),
- to protect digital infrastructure (digital infrastructure is the equipment, systems, places, information, people, networks and processes that are essential to the functioning of the country and on which everyday life depends, and also includes some functions, places and organizations that are not critical to the maintenance of essential services but which need protection because of the potential danger to the public),
- to protect animals (animal cruelty is an act of social terrorism, as animals are an integral part of modern civilization, not only in personal or professional life, but also in public life).

No member of the Digital Safety Council - DWO may ever act contrary to the principles of the Digital World Organization, the mission of which is:

- protecting the virtual world from GLOBAL (security, social, health, economic, environmental and cyber) THREATS,
- protecting the digital civilization made up of citizens of all nations,
- protecting the digital law, which will be legally binding for the DWO member states, the
 digital law is a set of generally binding rules of conduct of the digital civilization in the
 virtual world,
- protecting the digital charter of rights and freedoms, which will be legally binding on the DWO member states.

- protecting the digital sovereignty of the DWO member states,
- protecting the digital identity of the citizen homo digitalis,
- protecting the cyber economy on which the national economies of the Digital World Organization member states existentially depend,
- animal protection (animal cruelty is an act of social terrorism, as animals are an integral part of modern civilization, not only in personal or professional life, but also in public life).

Members of the Digital Security Council - DWO have a staff of international officials who are responsible only to them and not to governments.

Should any member of the Digital Security Council - DWO act in contradiction to the principles of the Digital World Organization, then it is the legal duty of the DWO Digital Assembly to call a vote for immediate removal from office.

Should any member of the Digital Security Council - DWO act in contradiction to the principles of the Digital World Organization, a supermajority in the Digital Assembly is required to remove them from office immediately.

The Digital Security Council - DWO will hold a regular annual Global Cyber Peace Summit the purpose of which shall be:

- protecting the virtual world from GLOBAL (security, social, health, economic, environmental and cyber) THREATS,
- protecting the digital civilization made up of citizens of all nations,
- protecting the digital law, which will be legally binding for the DWO member states, the
 digital law is a set of generally binding rules of conduct of the digital civilization in the
 virtual world,
- protecting the digital charter of rights and freedoms, which will be legally binding on the DWO member states,
- protecting the digital sovereignty of the DWO member states,
- protecting the digital identity of the citizen homo digitalis,
- protecting the cyber economy on which the national economies of the Digital World
 Organization member states existentially depend,
- animal protection (animal cruelty is an act of social terrorism, as animals are an integral part of modern civilization, not only in personal or professional life, but also in public life).

The Global Cyber Peace Summit is a key performance indicator for the Digital World Organization, which conducts an assessment of progress, success, failure or success for each past year in the fields of:

- protecting the virtual world from GLOBAL (security, social, health, economic, environmental and cyber) THREATS,
- protecting the digital civilization made up of citizens of all nations,

- protecting the digital law, which will be legally binding for the DWO member states, the
 digital law is a set of generally binding rules of conduct of the digital civilization in the
 virtual world,
- protecting the digital charter of rights and freedoms, which will be legally binding on the DWO member states,
- protecting the digital sovereignty of the DWO member states,
- protecting the digital identity of the citizen homo digitalis,
- protecting the cyber economy on which the national economies of the Digital World Organization member states existentially depend,
- animal protection (animal cruelty is an act of social terrorism, as animals are an integral part of modern civilization, not only in personal or professional life, but also in public life).

DIGITAL COURT

One of the key bodies of DWO is the Digital Court, to which individuals, legal entities and member states can turn.

If individuals, legal entities and member states apply to the Digital Court, they are obliged to honor and respect its judgment, which is final and irrevocable.

However, the digital court also carries out criminal proceedings, which are regulated by the digital law, the aim of which is to determine whether a crime (e.g.: social terrorism, cyber-terrorism, etc.) has been committed in the virtual world, to identify the perpetrator, to impose a penalty or protective measure on him/her under the digital law and to enforce this decision or ensure its execution.

In addition to the law enforcement authorities, other persons participate in criminal proceedings and, depending on their position in the proceedings, have different rights and obligations. The aim of criminal proceedings is also to prevent crime in the virtual world and to act as a preventive measure for citizens.

The Digital Court will operate in each member state and will have as many judges as needed. The individual judges are elected by the Digital Assembly.

If anyone involved in the case fails to comply with the judgment in any way, then the DWO member states are obliged to file a complaint with the Digital Prosecutor's Office for circumvention of the enforcement regulation and violation of the Digital Act.

DIGITAL SECRETARIAT OF DWO

The Digital Secretariat of the Digital World Organization will carry out the day-to-day activities of DWO as mandated by the Digital Assembly and other bodies of the Organization as appropriate. The secretariat is headed by the Digital Security Council - DWO and has staff all over the world. The Secretariat is organized according to the DWO statutes, with offices and departments coordinating with each other to ensure consistency in the DWO work programme.

CHANCELLOR OF DWO

The Chancellor is a diplomatic title for the highest ranking member in the DWO hierarchy who has decision-making powers and is responsible for the running and functioning of the Digital World Organization.

The Chancellor has at his disposal administrative representative premises, a large staff, security, official vehicles, diplomatic facilities in each country and many other necessary means to handle and control all matters and activities throughout the DWO.

The Chancellor of the Digital World Organization shall only be a person who has demonstrated deep skills and knowledge in the running and functioning of the DWO and has a forward-looking vision to dynamically develop the DWO's activities in the digital age in the following fields:

- building digital peace,
- protecting the digital civilization made up of citizens of all nations,
- protecting human rights and freedoms and the duties of man,
- protecting the cyber-economy on which national and global politics depend.

In addition to administrative matters, the Chancellor presents forward-looking visions for the development of DWO activities in the digital age to the Digital Assembly, the Digital Security Council and the President of DWO.

The duties of the Chancellor are given by the Digital Order.

Digital Policy Institute - millennium 3000 Ladislav Boldi www. digital policy in stitute. digital