10.12753/2284-9378-20-32

UPDATING LEGISLATION IN THE FIELD OF NATIONAL SECURITY – ADAPTING TO THE NEW REALITIES. NEEDS AND CHALLENGES

Georgian POP*

Romanian legislation specific to the national security is, at a great extent, quite obsolete. The laws were established in the 90s' and are submitted to the logic specific to the Cold War. In the meantime, not only the crisis generated by COVID – 19 but also the technological and geopolitical evolutions which appeared during the latest decades have emphasized the need to adapt the laws to the new realities. Comparing the situation specific to the three decades before, new security risks have shown up, for example cyber risks. The New Defence Strategy of our country (the one of 2020), emphasizes the keen need to update these laws.

The great challenge for the legislative initiative consists in finding a right balance between the need to prevent/counteract these risks, on the one hand, and, on the other hand, the need to protect the fundamental freedom and to assure the care to respect the constitutional rights of the citizens. The lack of this balance can open the way either towards abuse against the citizens or towards institutional inefficiency. Consolidation of democracy and state are dependent, greatly, on the content of these laws.

To have a legislation that is modern and adequate, adapted to the democratic environment, the principle of constitutionality (namely to protect the citizens' freedom and fundamental rights), must be the base of the legally regulation specific to new security risks.

Keywords: security; legislation; risks; challenges; adaptation.

An analysis of the factors that have led to changes and improvements in legislation over time is a fascinating journey into universal history. If in legislative theory and practice certain concepts and principles have remained valid from antiquity to the present, the actual content of the laws has undergone, in each historical stage, consistent changes.

At higher or lower speeds, war and peace, the crises that humanity has gone through, scientific discoveries, technological inventions and innovations, geopolitical dynamics or social developments have shaped every historical period. Adapting laws to these developments has always been both a necessity and a challenge for the legislators of all times.

In recent decades, technological developments have been spectacular, influencing the economy, industry, politics, scientific research, entertainment, lifestyles, social interaction, etc.

For example, 30 years ago we considered science-fiction the smart phone technology that we use today, on a daily basis, in a natural way. As a result, the pace of political, economic and social change has been accelerating.

**** Member of the Romanian Parliament***
e-mail: *georgianpop75@gmail.com*

In recent decades, technological developments and geopolitical dynamics have made security risks increasingly complex. Practically, there have never been such evolutions and challenges in history, hard to imagine a few decades ago. Cyber risks, the use of drones to cause security incidents, hybrid warfare and, in general, new asymmetric risks have not been defined in specific national security legislation.

The crisis generated by COVID-19 has highlighted, in addition to the developments of recent decades, the need to update legislation. Innovative technologies (robots, drones, IT applications, etc.) have facilitated human action and, implicitly, pandemic management. By comparison, 100 years ago, during the pandemic known in history as the "Spanish flu", no one could have imagined that robots could disinfect hospitals, that drones could deliver drugs to areas at risk to humans, that mobile applications could be used to identify the social interaction of infected people. But obviously, the use of new technologies can be dual, depending on the user's intentions: in addition to the benefits, new technologies can be used to limit fundamental rights and freedoms.

From saving lives to abusing fundamental freedoms, there is, in some cases, a very fragile line that needs to be regulated, correctly and precisely, within a law. If laws are not clear enough, committing abuses undesirably falls into the realm of human arbitrariness.

The need to update legislation

One of the great challenges for Parliaments, not only in Romania, but in most countries of the world, is related to the adaptation of security legislation to recent developments, including the developments generated by the COVID-19 crisis.

Romanian legislation was drafted and adopted in the 1990s[1]. In general, the logic specific to that period was a "cold war" type, the main security risks being military aggression, espionage, terrorism, hostile actions, spreading false information, propaganda for war, risks of secession, diversion, attacks against constitutional order etc.

The last three decades have brought significant changes. If, for example, 30 years ago we would have defined a military aggression mainly in conventional terms, today an aggression against a state/community can be of the cyber type. That is, instead of classic tanks, an attack can be made in the virtual environment, with weapons from the cyber arsenal, to destroy or paralyze certain critical infrastructures. The effect produced, political and military, is, in most cases, comparable to the damage caused by conventional weapons. Espionage has changed a lot. If during the Cold War states sent their spies to obtain secret documents and information, today it can be done through cyber tools, remotely, not just through agents sent to the scene.

If in the '90s the potential aggressors were mainly state entities or terrorist organizations clearly defined, relatively easy to identify, today we face a series of diffuse, asymmetric, unconventional threats, whose perpetrators are more difficult to identify and counteract: troll factories/farms, hackers, lone wolves who self-radicalize on social networks and commit terrorist attacks, etc. For these new risks, the legislation drafted 30 years ago does not provide definitions and legal frameworks.

Prevention is the golden rule of modern intelligence. Let us take espionage as an example. Effective prevention means manipulating and hijacking spies of a hostile power in order to fail to obtain the secret information they are targeting or to fail to recruit / influence important leaders. If the espionage / betrayal action took place, prevention failed. Even though the court later convicts the culprits, both spies and traitors, the damage is done. The same is true for terrorist attacks. Prevention means that any attempt is thwarted, blocked, pre-met, that is, the actual attack does not occur there are no human victims and destroyed infrastructure. It is preferable for terrorists to be blocked, expelled, pre-trial detained than to be tried and convicted after committing attacks, because in such cases prevention means saving lives.

Current legislation provides the legal tools needed to prevent/counter classic risks such as espionage or terrorism. But it does not cover new risks, such as "troll factories", for example, used by a hostile power to create diversions and destabilization.

A simple reading, in 2020, of the Romanian legislation in this field reveals that security risks have evolved and diversified while the legislative provisions have lagged behind these developments. Obsolete and inadequate legislation represents intrinsically a vulnerability as it does not provide the legal tools to prevent and counteract these risks.

Challenges for the legislative process

The fundamental role of legislation is to adequately regulate all areas of social life. From the perspective of national security legislation, we currently have some major challenges.

A first challenge concerns the exhaustive dimension of the future legislative package so as to cover the great diversity of risks that have occurred in recent years. It is thus necessary to supplement the list of national security risks by including those that have occurred in recent decades. The approach must be balanced, in order to avoid both the evading of real risks and the abusive, forced introduction of some security risks.

Secondly, a significant challenge associated with the legislation in this field is the observance of the principle of Constitutionality, namely finding the right balance between, on the one hand, the need for efficiency in ensuring national security (meaning risk prevention) and, on the other hand, protecting fundamental human rights and freedoms.

How do we draft new legislation to enable us to maximize the benefits of IT&C technology (legislation should not be a brake on development)

and at the same time to minimize the risks of these technologies being used as a weapon against citizens, communities or states? How do we draft new laws to avoid the possibility of governments illegally spying on their citizens through these technologies?

Thirdly, the COVID-19 crisis management revealed to us the possibility, practiced in some states, that espionage technologies, used for monitoring and surveillance, could be used, in the name of medical security and stopping the spread of outbreaks, to mass surveillance of citizens[2], implicitly generating an interference in the sphere of the right to privacy.

The legislative challenge is extremely complex. Is a pandemic a sufficient reason to legislate for the use of mass surveillance technologies? Such as, for example, the obligation to install the STOPCOVID application on personal smart phones? The French Parliament legislated this obligation in 2020[3].

What is the limit over which the damage of democracy and fundamental freedoms becomes irreversible? If such IT applications are approved for pandemic management (COVID-19), are there sufficient reasons to extend their use to combat terrorism, for example, cyber espionage or hybrid warfare?

Without a clear and responsible regulation, we can witness in the future extreme phenomena, either the non-optimal use of technological resources for risk management (a pandemic, for example), or the "overuse" of technological resources for illegitimate monitoring of citizens (governments or private companies).

COVID-19 and its implications for national security

If until the outbreak of COVID-19 the main paradigm of approaching national security laws sought the balance between civil liberties and national security, the pandemic changed the concepts of reference, this time the discussion being about finding a balance between public health and fundamental freedoms. In France, for example, the legalization of the use of the STOPCOVID application on smart phones is eloquent for the relevance of the new paradigm.

An analysis of the measures adopted or proposed in various countries around the world for the use of mass monitoring technologies for pandemic management reveals that the challenge for national parliaments is extremely complex.

According to the Treaty on the Functioning of the European Union, national security legislation is an area of national sovereignty. Therefore, in the EU area, each state will have to decide on the specific form of transposition of these challenges. From state to state, some technologies will be allowed, others banned. For example, unlike France, in Romania there is no question of legislating the obligation to install the STOPCOVID application on personal smart phones.

In addition to the applications installed on citizens' smart phones, some states, under the motivation of protecting students, have imposed the mandatory wearing of electronic bracelets in schools, used to manage social distance and to issue warnings if a student has a fever[4]. In another state, the idea of implanting chips for students was launched, the motivation being to protect students from the danger of COVID-19[5]. The Spanish company Herta Security is developing a complex facial recognition system in public spaces, including under the conditions of wearing a medical mask[6]. The French company Outsight is developing a laser-based system that will allow the management of social distance in public spaces[7]. Drones or special helmets worn by police officers[8] can be equipped with cameras that scan, in real time, the temperature of people in public spaces. Some of these technologies are, in various states, approved by law and applied. Others are only in the proposal / project stage.

Sooner or later, Parliaments will have to address these issues in each state. The challenge is obvious. Does it regulate or NOT the possibility of using such technologies for the purpose of COVID-19 pandemic management? If so, under what conditions? Who manages such technologies? Who exercises democratic control so that there are no abuses or uses of technology for political, commercial, etc. purposes? If such technologies can be used to save lives in the face of the danger represented by the pandemic (COVID-19), could the same technologies be used to save lives in the face of the terrorist danger? What about saving / protecting critical infrastructures from cyber or hybrid risks? Where is, in this case, the right balance between freedom, the right to privacy, on the one hand, and the protection of public health or the protection

of the lives of citizens, the protection of critical infrastructures (health, energy, communications), on the other?

Another topic related to the impact of the COVID-19 crisis in the field of national security concerns the involvement of the secret services in the national effort to manage a pandemic. In Israel, for example, the secret services have become heavily involved in commercial actions to bring to Israel millions of medical equipment items needed for COVID-19 management, including from countries with which Israel has no diplomatic relations[9], the secret services (Mossad) receiving official congratulations for this involvement[10]. Is such involvement legitimate? What solution will we establish in the Romanian legislation? Who determines what types of trade/economic implications are legitimate or illegitimate? Who controls the possible exceeding of the national security mandate in such a case? Do we prohibit/ allow secret services to conduct commercial activities? To all these questions, the new legislative package will have to find the right answers.

Another topic of public controversy was the information provided by the secret services to policy makers about the dangers of COVID-19. In the US[11] and in the main EU countries, this topic was raised in the public debate: how do we establish, through legislation, the task of the secret services to inform, in advance, policy makers about pandemic risks and how do policy makers use information to generate public measures / policies for the proper management of a pandemic?

The evolution of security risks in recent decades

Because we are living the fourth industrial revolution[12], even more, we are at the beginning of the fifth[13], updating the legislation means, in the simplest form, adapting to the new world defined by virtual and smart technology.

In addition to technological developments, significant influences on new security risks have also had the recent geopolitical developments: the annexation of the Crimean Peninsula by the Russian Federation, political and military developments in the Middle East or North Africa, migration pressures on the EU or the latent tensions in the South China Sea.

Without claiming to be exhaustive and without trying to suggest certain solutions, I have chosen, to exemplify, some of the new security risks, trying to highlight the legislative challenges that are associated with each of these new risks.

Hybrid warfare

Thirty years ago, discussions about a hybrid war would have been predominantly theoretical. Meanwhile, after the Russian Federation annexed Crimea, the hybrid warfare became a real political-military phenomenon. Hybrid attacks are an extremely effective combination of cyber-attacks, actions of special troops without insignia and not assumed by states (the famous "green men" in Crimea, for example), hostile propaganda, fake news campaigns, stimulation of minorities or extremist groups in a region to generate instability and claim certain political goals, use of energy and economic levers, etc.

The objectives pursued by the hybrid warfare aim at social destabilization, the collapse of public confidence in legitimate authorities, social tensions and conflicts, the massive influence of public opinion to generate a "strategic paralysis" of policy makers, meaning the inability to make decisions. The weapons used in hybrid wars are no longer tanks or missiles but cyber "weapons", fake news campaigns, hostile propaganda, energy levers, etc.

In the new national security legislation and, subsequently, in the chapter of the criminal code that defines the crimes against national security, this phenomenon (hybrid war) must be defined separately.

The legislative challenges are many. First, how do we define the enemy in hybrid incidents? More precisely, how do we define, in order to be able to legally frame, such phenomena as hostile propaganda or fake news through social media, coordinated by a hostile state entity? How do we legally frame "green men", not assumed by any state, or mercenaries of armies/private companies[14]? How do we legally define "troll factories" in another state as a risk to national security? How do we establish that an extremist group or a minority is being manipulated by a hostile foreign power to generate local tensions and conflicts? How do we legally define, in terms of a possible instrument of hybrid aggression, the energy security?

Secondly, we will have to assess the extent to which an incomplete or exaggerated definition of these phenomena can lead to abuses regarding

fundamental rights and freedoms. It is very important for the state to have, for example, the necessary tools to counter a fake news campaign orchestrated by a hostile power against its strategic interests. During the COVID-19 pandemic, in the spring of 2020, Romania was the target of such hybrid campaigns. The Minister of Internal Affairs of Romania officially confirmed it[15].

But it is equally important that such tools cannot be used to affect freedom of expression in a democratic society. How do we achieve, through the legislative provisions, both desires, namely how do we find the right balance?

Thirdly, we will need to identify and define the optimal mechanisms for inter-institutional cooperation. More precisely, to establish, through legislation, the distinct but competing responsibilities for the army, police, secret services, border police, gendarmes, etc. For example, on May 10, 2019, a small helicopter, used by cigarette smugglers, crashed in northern Romania[16] in a forest and was found, by chance, 3 days after the crash by some locals. We are obviously wondering how it is possible for a hard device to enter, undetected, in the airspace of Romania? And of course, from the perspective of a possible hybrid aggression, we ask ourselves what would have happened if instead of contraband cigarettes that helicopter introduced "green men" on the national territory? Which institution is responsible for such incidents: the army, the border police, the gendarmerie?

Clearly, the new legislative package will have to legally regulate all these phenomena and situations, including institutional responsibilities for preventing and counteracting them. The case of the helicopter discovered, by chance, on May 10, 2019 is eloquent. No institution has officially assumed this failure and no institution has officially proposed a set of measures to prevent the recurrence of such an incident.

Cyber risks

In the last 2 decades, the development of IT&C has been practically exponential. As a result, the quality of life, social and community development, research, medicine, the financial-banking sectors, transport and infrastructure have undergone developments hard to anticipate 20 years ago.

Undoubtedly, the life of the contemporary man can no longer be conceived outside the Internet and IT technologies. The positive effects are found both at the individual level and at the community and societal level. But in addition to obvious benefits, the development of IT & C technologies also involves a number of risks. The protection of personal data takes on a new dimension in the information age. For example, the medical data of the citizens were kept, 30 years ago, on paper, in the doctors' drawers. Now most patient data is stored and managed electronically. It is obvious that no patient would want his medical data to be accessed by hackers.

Educational systems are evolving. The students' homework are no longer exclusively the classic ones, from the textbook/notebook. The crisis generated by COVID-19 meant that, for several months, the school was run exclusively online. Students received virtual assignments, solved them and virtually submitted the answers. The classroom application[17] is an example. Obviously, no parent would want their children's confidential data on school performance to be accessed by unauthorized persons.

I used these examples to highlight the fact that, in the process of social development, IT technologies have a bivalent nature, both as a factor generating progress and as a vulnerability, a risk to national security or to the interests of communities, families and individuals.

The future is moving us towards smart cities[18] and smart societies. Digitization is undoubtedly the future of administrative systems. The benefits induced are obvious. It is only a matter of time before states manage to go through all the technical steps of digitization. Estonia, from this point of view, is a model[19].

But, in addition to the obvious advantages, the last decade has shown us that the cyber domain can also be used as a strong weapon. If, classically, the military confrontation spaces were the air, the ground and the sea, from the NATO Summit in Warsaw, in 2016, cyber officially became, inside the Alliance, the fourth military confrontation space.

The examples of the last decade are eloquent. In 2010, an innovative cyber virus, Stuxnet, was used to attack the computer systems of Iran's nuclear facilities[20]. The effect was to block the development pace of the Iranian nuclear program. Thirty years ago, only a special forces operation or a classic type of sabotage could have produced such

an effect. But Stuxnet, a computer virus launched from a distance, difficult to identify and attribute, produced the expected military and political effect. The cyber "response" is known as the Shamon virus. In 2012, this virus, Shamon, was launched on the computer systems of the Saudi state company ARAMCO, in the field of oil processing and on some refineries in Qatar. The cyber-attack caused major damage by compromising the data in the attacked computer systems, which generated a substantial slowdown in oil production, requiring a complete reconstruction of these computer systems[21].

Nor are civilian critical infrastructures, such as distribution networks for the population, protected from cyber risks! For example, in April 2020, Israel's water supply systems were affected by a cyber-attack[22]. In the classic military action, for example, in order to destroy the distribution of electricity or drinking water supply of a city, the effective ways were the bomb / missile attack on the network nodes, the attack with special troops to detonate the network.

Cyber weapons have shown that the same thing can be done remotely, without any classic explosions, by simply sending computer viruses. It happened on December 23rd, 2015, in the midst of the hybrid war in Ukraine, when the computer systems of electricity distribution companies were attacked and paralyzed[23]. The politico-military effect was great: the population remained in darkness in the middle of winter.

The major concern for the protection of critical infrastructure is that a cyber-attack can compromise and affect the operation of industrial facilities by attacking voltage, pressure and temperature control systems. From this point of view, thousands of industrial plants around the world are vulnerable, including nuclear and water treatment plants, oil or gas refineries, chemical plants, etc. Similarly, computer systems that manage passenger traffic (airports, railway stations, road traffic management systems, etc.) can be a target for cyber-attacks.

The big problem, in such cases, is the precise identification of the attacker. They usually are hackers that do not assume the facts and that are unrecognized by states, even if they act on command and in the interest of certain states.

It is difficult to define and frame such an attack in national or international law. And especially, the attacker. Because the attacker uses proxy servers, proxy routers, anonymous VPNs. This is, intrinsically, a major challenge for the drafting of new national security laws. How do we legally define and frame such an aggressor?

The development of cyber technologies has revolutionized espionage. If a few decades ago the access to the secret documents of a state entity was made by classical methods, such as "James Bond" or the recruitment of people who had direct access to documents, now IT technologies allow digital[24] espionage, through software or computer viruses, such as Pegasus[25] or even through antiviruses installed for the computer protection[26] of various IT systems. Generally speaking, states / secret services no longer have to send their own "James Bond" on a field mission. Some data can be collected remotely, digitally, identifying and assigning the attack being a difficult process.

Not only classified data of states are a target in cyberspace. Public health system data, banking and financial system data, digital procurement data and, in general, digital government data are vulnerabilities that need to be protected and secured. In 2020, a massive e-mail cyber espionage campaign fraudulently used big companies' names (Romanian Post, Banca Transilvania, DHL, etc.) as bait for users to influence the opening of emails containing spyware, the target being the theft of information from computers belonging to various public institutions in Romania[27].

From a legislative perspective, the main challenge is to find the right balance between, on the one hand, stimulating the digitization process at institutional, community, societal level and, on the other hand, establishing by law the rules and the level of cyber protection, so that digital data are effectively defended and, at the same time, fundamental rights and freedoms are protected.

What additional legislative tools do we offer to cyber defence agencies in order to be effective but, at the same time, not to become abusive, in relation with the citizens? Will we impose by law, as a measure to prevent cyber risks, mandatory rules/ levels of cyber security to various institutions, such as, for example, health insurance companies, public/private hospitals, banking institutions, local public administration, etc.?

Another challenge arises from the need for more efficient regulation of "dark" spaces in the

virtual environment. How do we legally define and frame traffic activities from the dark internet area (trafficking in drugs, weapons and prohibited materials, etc.)? Can server owners who deliberately host specialized sites for cross-border organized crime actions be incriminated or not? The recent case of a cyber bunker in Germany is eloquent[28] and will be an important case for legal regulation trends in the European Union.

Last but not least, will we legislate, in the new package of national security laws, the right of the government, the army or the secret services to cyber-attack the aggressors they face? In November 2019, for example, EUROPOL and the Belgian police cyber attacked hundreds of accounts promoting Islamic State jihadist propaganda[29]. Will we give the permission, in the new legislation, to the Romanian state institutions to carry out cyber-attacks or will we limit the intervention explicitly in the sphere of cyber defence?

Terrorism in the digital age – the phenomenon of self-radicalization on social media networks

Technological development has allowed the emergence of new forms of manifestation of the terrorist phenomenon. A few years ago, states and intelligence agencies knew very clearly who the enemy in the sphere of terrorism was: terrorist organizations/groups, from all over the globe, there was a clear index of them and mercenaries like Carlos "the jackal"[30], who put themselves in the service of the interests of some states or terrorist organizations. The attacks involved hijackings, bombings, gun attacks, and more. Prevention consists in monitoring the organizations /mercenaries, arresting, expelling the attackers, counteracting/annihilating the intentions to carry out the attacks. Obviously, all these classic risks have remained as real as possible and are still valid.

But the development of technology and social media has generated new possibilities for the manifestation of the terrorist phenomenon. If in the past the recruitment and radicalization of those who later actually committed the attacks was done directly, by terrorist organizations, now we have cases of self-radicalization through social media and virtual communication with the leaders of terrorist organizations. Therefore, it is no longer necessary to have an effective meeting between the leaders of terrorist organizations and the persons who, as a result of radicalization, become bombers. As an effect, in such cases prevention is much more difficult to achieve.

In the past, many attacks have been prevented by effectively monitoring the circuit of the explosives, the weapons to be used in the attacks, and the specific activities of terrorist networks / organizations. If a few decades ago bombs or firearms were the main weapons used by terrorists, the attacks in recent years, committed in Europe, have shown that the weapons used can be simple knives[31] or trucks with which the bombers enter the crowd of people on the street, as happened in Nice[32].

A suggestive case for the phenomenon of self-radicalization is the attack on December 6th, 2019, from the military base in Pensacola, Florida. A young Saudi man killed 3 people and injured another 8. The investigation launched, showed that prior to the attack, the young man posted anti-US and anti-Israel messages[33], on social networks.

The legislative challenge is obvious. Could a possible monitoring of the content posted on social media by the attacker have prevented the death of innocent people?

By contrast, on June 6th, 2020, in Germany, the police and the secret services arrested a young Islamophobic man who stated, in a post on social media, that he was going to commit an attack in a mosque, on the model of the Islamophobic attack in New Zeeland from 2019[34]. He failed to commit the attack because the police arrested him, based on the intentions posted in the virtual environment. The weapons with which the attack was to be carried out were found at the young man's home.

Analyzing the two cases, we ask ourselves the legitimate question where is, in such cases, the right balance between prevention and freedom of expression?

Certainly, an over-regulation of the possibilities of prevention would lead to an authoritarian state, to abuses and violations of the right to privacy and opinion, guaranteed by the Constitution! At the same time, life is the supreme human value, the right to life being fundamental! How can governments better protect the lives of innocent citizens who fall victims to theological radicalism without turning into Orwellian-type "Big Brother"?

The pandemic generated by COVID-19 marked a strategic mutation in the activity of terrorist organizations. Specifically, we are witnessing

a significant shift of actions from real space to the virtual environment: jihadist propaganda, the recruitment of new members and followers, the organization of attacks whose target tends to increasingly target cyber-attacks on critical infrastructure. ISIS / DAESH launched, for the first time, in 2020 the online magazine "Security of the supporter", whose content teaches members and followers of the organization how to avoid / circumvent the surveillance of information services in the online environment[35].

An ancient principle seems to retain its relevance even in contemporaneousness: "Laws given in time of peace are largely annulled by war, and laws given in time of war are annulled by peace"[36]. The big challenge is to find a balanced legal form, so that there is good legislation, drafted in peacetime, to maintain peace, democracy, fundamental rights but also to prevent the horrors of war, in this case the horrors of terrorist attacks.

Using drones as a weapon

In recent decades, the development of drone technologies has been spectacular. As a result, governments, private companies or citizens now have access to a diverse range of drones. In addition to the obvious benefits of transport, trades, and the entertainment industry, recent years have shown that drones can also be used as real weapons[37].

A major incident took place in December 2018, in London[38]. Gatwick Airport was blocked for 32 hours, and more than 100,000 passengers were stranded at the airport. The cause of the planes retaining to the ground was generated by unidentified drones that constantly flew over the space close to the airport runways. Although major police and military forces tried to identify the perpetrators of the incident, drones reappeared near the airport whenever an attempt was made to reopen the runway. The immediate solutions launched by the London authorities fell within the scope of operational reactions: the deployment of snipers to immediately shoot down drones, intense interference in that area, to block the possibility of remote drone control, with the risk of affecting other activities in the airport area or the launching of especially trained birds to shoot down unauthorized drones from the runway space.

Another drone incident in 2019 reveals the high potential of this technology to be used as a weapon. On September 14th, 2019, Saudi Arabia's oil industry was attacked by drones, which set fire to the facility[39]. The estimated damage was in the hundreds of millions of dollars and production was partially halted. Although Saudi Arabia has invested heavily in missile defence systems and, as a result, all missile attacks launched by Yemeni Huthi insurgents on Saudi Arabia have been countered, a much cheaper technology, drones, has been used by insurgents with a real success, as an extremely effective weapon, impossible to detect, by radar systems, and to neutralize by activating anti-missile systems.

If 30 years ago there was no question of defining drones as a national security risk, recent incidents are certainly forcing us to think and insert, in the national security legislation, a distinct point regarding drones. In addition to military-type destinations, drones can be successfully used by drug traffickers or arms traffickers, by transnational organized crime networks to transport illegal products across state borders.

Also, images from China, during the COVID-19 epidemic, showed the technical possibilities by which the population is monitored in real time with the help of drones and, at the same time, the population can receive, through megaphones installed on drones, directly and personalized, messages or summonses/instructions of conduct in the social space[40].

Thus, first of all, a legislative challenge will be related to setting the limits within which drones can be used by governments for population surveillance or in public order actions. Where is the right balance between the need for governments to use modern technologies (drones) to prevent criminal or antisocial phenomena, on the one hand, and, on the other, the right to privacy and the protection of fundamental freedoms? Where is the limit over which their use turns into abuses and violations of civil rights and freedoms?

Secondly, although European legislation regulating the use of drones has been improved[41] and in Romania we have a new Aviation Code[42], the challenge for national legislation in the field of security remains: how do we legally define and classify drones among national security risks? How do we protect ourselves from possible drone attacks? What are the institutions responsible for preventing and countering possible drone attacks

on critical infrastructure? How do we manage, through legislation, to protect the legitimate rights of citizens and companies that use drones for civilian purposes, for development? How do we prevent the use of drones for criminal purposes without affecting the development of this industry, through over-regulation?

Influence of election results by hostile state entities

The constitutions of all democratic states enshrine the right of citizens to elect their representatives and decide by referendum in a sovereign manner. For governments, one of the fundamental tests of democracy is the ability to hold free and fair elections/referendums so that the sovereign will of nations is not altered or manipulated by hostile state entities.

Throughout recent history, for geopolitical reasons or to promote strategic interests, there have been situations in which state entities have tried to influence, for their own benefit, the results of electoral processes in the countries concerned.

Democratic states have begun to present official positions[43] and reports[44] on such external interference, and the institutions responsible for defending the Constitution are developing strategies to counter external interference in electoral processes[45].

Commissions of Inquiry of such interference have recently been set up in the United States[46], the United Kingdom[47] or the Russian Federation[48]. This concern is also very current in the European space. We therefore have a motion for a resolution, submitted in October 2019 in the European Parliament, on external electoral interference and misinformation in national and European democratic processes[49].

An official US reaction is conclusive to show the size and the topicality of this type of risk. To prevent external interference in the electoral process, the US officially offers substantial rewards of millions of dollars to anyone who helps identify foreign actors who, at the command of foreign governments, are trying to influence the November 2020 presidential election[50].

30 years ago, for example, the influence of the result of the elections/will of the population in a sovereign state by a foreign (hostile) power could be done by classical means: secret financing of certain parties/leaders, of extreme or minority groups, of some organizations that promoted a certain agenda, the corruption/recruitment of some political leaders or of some opinion formers, etc. The actual results were, in such cases, relatively limited.

Today, IT technologies and the global development of social media networks allow the intentions to influence public opinion and, implicitly, the outcome of elections to be achieved, at least theoretically, remotely.

"Troll factories" can generate and launch in the virtual space real campaigns based on fake news. Computer algorithms and search engines can theoretically direct a series of manipulation/ misinformation messages to a well-targeted audience in a country/region/community.

Controversies over the role that Cambridge Analytica played in the Brexit phenomenon[51] are relevant. Thus, the company Cambridge Analytica was accused of using for political purposes, without consent, the personal data of over 50 million Facebook users[52]. What political parties have failed to achieve, through traditional means (classic election campaign methods), algorithms and software, Cambridge Analytica seems to have succeeded in doing. Specifically, 3,000,000 citizens who never voted were persuaded to go to the polls with more than 1 billion personalized messages sent through social media, based on users' personal data[53].

It is not the purpose of this article to determine whether or not the involvement of Cambridge Analityca was decisive for the success of the "Leave" camp in Brexit. But if we look at the results at the polls, where the difference was in the margin of 2%, and 3 million citizens went to the polls for the first time, some conclusions can be drawn.

The main idea I want to emphasize is that current technology allows the generation of tools to promote election campaigns that did not exist 30 years ago.

Specifically, through the traditional election campaign tools (door-to-door campaigns, distribution of election materials, public events, mobilization of supporters, etc.), available to political parties, it is impossible to generate personalized messages for millions of people! In order to deliver personalized messages to several million people through classic electoral mechanisms, the electoral campaign teams (documentation / creation / distribution) should include thousands

and even tens of thousands of members. And this is impossible for any political party in the European and Euro-Atlantic space.

But for a company that has the necessary software and computer algorithms, distributing personalized messages to millions of people becomes a real possibility.

The great challenge for national security legislation is to define and legally frame such a possibility for a hostile state entity to use such tools to manipulate, in its own interest, the sovereign right to choose of a nation/community and to generate legislative instruments so that any government can prevent such a situation.

In Spain, a Supreme Court judge has launched a judicial inquiry regarding the possible interference, through such instruments, by hostile secret services in the separatist process in the province of Catalonia[54].

How do we define and legally classify such phenomena within the national security risks?

Is there a risk that over-regulation will undesirably affect democracy and freedom of expression in a society? Definitely yes! Which institution should be given the legal responsibility to prevent and counteract such a risk? The Permanent Electoral Authority (PEA), the police, the army, the secret services? Do we need a new institution, specially created, to manage such phenomena? How do we establish, by law, the mechanisms of prevention? Where is the right balance between freedom of expression, freedom of communication, on the one hand, and, on the other, the protection of the nation's sovereign right to choose freely?

Hostile external propaganda and fake news campaigns

In any democratic regime, public support is essential for the consistency and coherence of government policies. All the more so when we talk about policies, projects and interests of a strategic nature. Romania's integration processes into NATO and the EU, at the end of the 1990s and the following decade, had an extremely important public support. The relevance of this support has translated into applied policy projects (legislative amendments and adoptions, public policies, institutional reform projects, etc.) that have made integration possible.

The theory of attitude change, from social psychology, tells us that at the level of public opinion significant changes can occur slowly but progressively, if the incentives to influence public attitudes are constantly transmitted to a target group[55]. A relatively recent example seems suggestive to illustrate this theory: the evolution of public support for EU integration by the population of the Republic of Moldova. If in 2007, in the Republic of Moldova, the supporters of European integration represented 76%, in 2014 only 44% still supported this project[56]. And the election results after 2014 have consecrated this trend.

Obviously, there is a causal complex responsible for reducing public support from 76% to 44%, and hostile propaganda (European integration) is one of the factors[57]. Certainly, the geopolitical beneficiary of this decrease is by no means the Republic of Moldova.

I have presented this example to illustrate the situation where a great geopolitical power can promote and transfer its specific interests in another state through fake news and hostile propaganda campaigns. Although the sociological method of content analysis can reveal relevant correlations between certain geopolitical interests and the actual content of hostile propaganda campaigns, in legislative practice the legal framework and proof of the "guilt" of hostile propaganda prove to be an extremely difficult endeavor. Often the line between information and misinformation, between propaganda and simple promotion (PR) is extremely thin. And the freedom of expression, the independence of the media, the freedom of communication in the virtual space represent fundamental rights that must be constantly defended and strengthened. The problem is that these very democratic principles and values can be exploited, in a professional manner, by the masters of propaganda that are in the service of hostile geopolitical powers.

As a result, a major legislative challenge will be to define this type of security risk and to define the institutional responsibilities for preventing / counteracting this phenomenon. At the same time, the establishment of the limits beyond which such an approach could turn into abuse on free expression or on the independence of the media, will have to be the basis for the elaboration of the new legislative provisions.

The fake news campaigns during the COVID-19 pandemic operated in the USA or the EU are eloquent[58]. The technical mechanism for promoting

a campaign involves the official media of a state, which launches a theme, then thousands of social media accounts (many of them fake) take the message in the languages of international circulation (English, German, French, Spanish, etc.) and massively promotes it on social media networks[59]. The fake news campaign against 5G, during the COVID-19 pandemic, was promoted through thousands of Facebook, Twitter and Instagram accounts, which produced thousands of posts with a huge reach during the state of emergency, with the hashtag # 5Gcoronavirus[60].

Obviously, the "weapon" of fake news aims to generate social instability, disproof and distrust in the legitimate authorities of a state. The ultimate goal is to block strategic decisions that geopolitically disadvantage the hostile state that promotes that fake news campaign.

Recent history reveals that the main method of combating fake news is the consistent education of the "target" population. The Finnish model proved to be, by far, the best[61].

"Finland is considered the European country most resistant to the phenomenon of fake news, as critical thinking is cultivated and stimulated throughout the educational process. Critical approach, interpretation, verification and evaluation of all the information you receive, from wherever it appears, are crucial. Finland's school curriculum is part of a broader strategy conceived by the Helsinki government after 2014, when the country was the target of a fake news campaign launched in Russia. In math classes, for example, students learn how easily statistics can be manipulated. In art classes they can see how easily the message of an image can be distorted, in history classes they analyze the most notable propaganda campaigns, while Finnish language teachers show them how many words can be used to confuse, to induce in error and deceive. Even if they do not read newspapers or watch TV news, students and citizens in general are bombarded daily with hundreds of news on WhatsApp, YouTube, Instagram, Snapchat, etc. The basic goal of the Finnish education system is for students and pupils to ask questions such as: who produced this information and why? Where was it published? What does it really say? What audience is it targeting? What is it based on? Is there evidence that this is the case or is it just someone's opinion? Can it be checked elsewhere?"[62]

Even if the fascination of the Finnish educational model tends to inspire us, the legislative challenge remains. With the exception of education-specific legislation, how do we define and legally classify, in the category of national security risks, hostile propaganda and fake news campaigns coordinated by hostile state entities? Because without an adequate definition and legal framework, any approach is completely useless; it can even become dangerous for the democratic environment! Which state institution receives such legal responsibility? How do we create control mechanisms so that we can avoid abuses on the independent media, freedom of expression or the right to an opinion?

The risk of legal over-regulation is real and can undesirably affect democracy and fundamental freedoms. The boundaries between these categories are extremely thin and history reveals many examples when demarches that started with good intentions were distorted and ended in deplorable abuses and dictatorial regimes.

Development of mass monitoring technologies, SMART networks, crypto currency, and AI (artificial intelligence)

The evolutions of digital technology and artificial intelligence (AI) tend to place us in a new stage, defined as the beginning of the *fifth industrial revolution*[63]. We are living through a period of huge transformations. Computers can work faster, better and more than humans, and integrating AI into this equation brings us to where robots and machines will be able to make decisions. This does not mean that robots will replace us but will be our partners in smart companies.

The future means that we will live in smart homes, we will move with smart means of transport, on a smart type of transport infrastructure, cities will change to become smart, institutions will transform and become smart, and interconnection will be done through smart connections (Smart Grids). It is a type of network that involves human cooperation with the computer and in which computers, based on advanced software, can make decisions. In a SMART city, communication and information are based on advanced technologies. Buildings, public transport systems, administrative and government services, commercial store networks, traffic management, etc. they all are coordinated and controlled by technologies such as AI (artificial intelligence) and IoT (Internet of Things).

Obviously, this technological-industrial revolution will stimulate development and will have positive effects on people's lives. The great legislative challenge is to properly regulate all these developments. Like any technology ever invented, bivalent use (for positive or destructive purposes) will be an explicit option for the user. That is why the legislation must adequately regulate all these situations: to stimulate positive developments and to counteract negative uses. Who protects new SMART cities/buildings from cyber-attacks? Can the IT department of a small town that invests heavily in SMART technologies cope with a possible cyber-attack launched by the "hackers" of a large (unaffiliated) hostile geopolitical power?

The controversies surrounding 5G technologies are eloquent. Are certain 5G devices security vulnerabilities[64]? How do we legally regulate such risks? Because there are new risks, non-existent a few years ago, so not regulated by the legislation in force. In 2019, we witnessed official accusations made by the US regarding the risks that the adoption of certain 5G technologies may present vulnerabilities in digital espionage[65]. Thus, a legislative challenge is to turn assessments, analyzes and statements/allegations of digital espionage risks into effective legal content, on the basis of which we can legally frame such technologies in the area of national security risks and thus have a legal basis for accepting or rejecting certain technologies. Otherwise, arbitrariness will play the dominant role.

Digital technologies have evolved a lot in the last decade. Facial recognition technologies can now be applied to populations of hundreds of millions of people, and in some states such procedures have become mandatory by law[66]. Obviously, governments, the police, the secret services will want the widest possible application of these possibilities, in order to quickly identify a large number of criminals, terrorists, criminals, prosecuted persons, violent criminals, etc.

Facial recognition even when wearing a medical mask, electronic bracelets, software installed on mobile phones (STOPCOVID, for example) are technologies not currently regulated by Romanian legislation. It is the role of the Romanian Parliament to establish, by law, which technologies can be allowed and which cannot, under what conditions they can be adopted and through what mechanisms democratic control is exercised over their use. In this case, the principle of Constitutionality applied in future legislation will have to represent the guarantee that the state institutions do not turn into real "Big Brother" [67]described by George Orwell in "1984" [68].

It is expected that, in the financial field, virtual currency, crypto currency, will occupy, progressively, as much space as possible in domestic and international transactions. LIBRA, for example, is designed to function as a new global payment system[69]. Obviously, it will be a while before the crypto currency plays a decisive role in the global financial system. But the trend is obvious. The question that arises, from a legislative perspective, is whether the regulation of processes involving crypto currency is done exclusively in legislation specific to the financial-banking field. Can we identify national security risks generated by possible speculative attacks using crypto currency as a tool? Or cyber-attacks with the aim of huge frauds? If so, how do we define and legally frame, in the content of the new legislation, the crypto currency among the national security risks?

It is already a common fact to say that AI (artificial intelligence) will revolutionize all aspects of social life, with exponential developments in medicine, transportation, communications, research, industry, entertainment, etc. After the consideration of the computerization, in the specialty literature, as a second literacy of institutions and human communities, it seems that AI is a new, higher level. AI (artificial intelligence) will increase, exponentially, the ability to calculate, analyze information or satellite images. In addition to civilian developments, AI military applications actually generate programs and projects with huge potential. Thus, used in the military and security fields, the role of AI is designed to improve, to prolong the possibilities of the human intellect, not to replace them. AI systems will integrate people and machines into a the partnership, which will lead to improved information gathering, processing and interpretation at higher parameters, improving the level of armies' efficiency, supporting decision-making processes and management of combat actions, but also to an exponential increase in the possibilities of virtual espionage, propaganda and the promotion of strategic interests through virtual tools[70].

Can we avoid the AI phenomenon in the debate on new national security legislation? How will we legally regulate Artificial Intelligence (AI) in general, and how will we define and frame AI in the list of national security risks? Where is the right balance between promoting and supporting AI for economic and social development, on the one hand, and the ability to prevent the use of AI as a weapon against the state, institutions, communities, or citizens, on the other?

Conclusions

The global security environment has changed a lot in recent decades. The general trend was marked by the emergence and development of unconventional, asymmetric and hybrid risks. Thus, the nature of war and aggression in general has changed. The war has not disappeared from the global geopolitical map. Only the forms of manifestation have diversified and become more sophisticated, making the most of the possibilities offered by technology. In the 21st century, a military aggression is no longer necessarily done with tanks, on the model of the 20th century. The aggressor can send a computer virus and the damage caused or the politico-military effect can be similar. If the owners of tanks (heavy military equipment) are relatively simple to establish, in the case of cyber-attacks the identity of the attacker is difficult to prove. Because the attacker usually uses proxy servers, proxy routers, anonymous VPNs.

An air attack is no longer necessarily done with airplanes or missiles, as they are clearly identifiable as belonging to a state entity. It can also be done with drones, whose cost is much lower and membership can be attributed to non-stable entities, of proxy type[71]. And the destruction produced should be just as great. If in the twentieth century states sent their special troops in various operations to attack strategic objectives, in the twenty-first century we have situations in which special troops operate without insignia ("green men" in Crimea and eastern Ukraine) or belong to private security companies, as it is the case in Syria[72], Libya[73] or in other areas of armed conflict[74].

Although the nature of the risks has changed, it is relevant to point out that the importance of classic risks remains high. More specifically, it is necessary for states to develop response and countermeasures for asymmetric and hybrid risks, but it is equally important to modernize their capabilities to counteract classic risks. It would be a great strategic mistake to minimize the importance of classic risks and threats. It would be wrong to invest exclusively in cyber defence, because at some point we might face tanks at the border. Therefore, the challenge for governments is to find a balance in the development of defence capabilities, between old and new, between classic and hybrid.

I tried to highlight the fact that the technological and geopolitical evolutions of the last decades have generated the need to modify the legislation in order to adapt it to the new realities. Recent history in the European and Euro-Atlantic area shows that changes in national security legislation have been made mainly in response to security incidents and terrorist attacks. It happened in the USA (Patriot Act adopted as a reaction to 9/11), France, Germany, Great Britain, Belgium. Basically, the legislative approach in this field was mainly reactive and not proactive.

In Romania we have not had significant security incidents in the last decades. For this reason, neither the public pressure to amend the legislation was high. There were initiatives and projects, but the successive political and electoral contexts were not likely to generate the completion of these legislative projects.

The main idea of this approach lies in the huge challenge that the Romanian Parliament has in the process of legally regulating the new security risks. The integrative concept will have to be the principle of Constitutionality, a principle that obviously represents the essence of any democracy. The need to prevent security risks and protect the lives of innocent citizens must in no way lead to over-regulation that generates abuse and oppressive behavior. History has shown us that the great dictatorial regimes based their existence and consolidation of power on ideologies presented as saving and liberating. It is just that practice was completely opposed to the theory and to the ideologies on which they were built.

The current approach aims to reveal these legislative challenges. Classic security risks remain a constant. It is just that governments have a long experience in dealing with them and parliaments have legislated these phenomena and there is legislative experience in this regard.

When addressing new security risks, legislative experience is extremely limited. We will have to innovate and produce definitions and legal frameworks for unregulated phenomena so far. Troll factories used by a hostile state entity as a weapon against our national interests, technologies that allow mass monitoring (software, applications, electronic bracelets, face recognition systems, etc.), cyber-attacks against critical infrastructures, self-radicalization in the virtual environment are some illustrative examples for the difficulty and complexity of this legislative approach.

As has been the case lately, the debate and adoption of new national security laws may be postponed sine die. In each parliamentary cycle, in the last decades, there were talks about the need to adopt new laws, but the approach remained strictly at the level of intention. It is very possible that in the context of the crisis generated by COVID-19 no one will take this step. Who assumes the legal regulation of the new security risks with all the legislative challenges set out above, especially in the electoral context?

It is possible to remain confined to the same paradigm of non-action. However, as time goes on, technological and geopolitical developments will generate processes and phenomena that are increasingly difficult to prevent and counteract based on legislative instruments developed 30 years ago. Outdated legislation is, intrinsically, a vulnerability.

We will evolve towards the SMART society as we adapt our legislation, mentalities and institutional practices to SMART challenges.

NOTES:

1 *L 51 /1991 – National security law*; *L 14/1992 – Law on the organization and functioning of SRI*; *L 1/1998 – Law on the organization and functioning of SIE*; *L 191/1998 – Law on the organization and functioning of SPP*; *L 92/1996 – Law on the organization and functioning of STS*; *L 535/2004 Law for preventing and combating terrorism*.

2 https://www.newmoney.ro/ce-tehnologii-de-supraveghere-folosesc-tarile-impotriva-coronavirusului-desi-o-parte-din-ele-afecteaza-anumite-drepturi-ale-omului/, accessed on 14.05.2020.

3 http://www.rador.ro/2020/05/28/parlamentul-frantei-a-votat-in-majoritate-pentru-aplicatia-stopcovid-pentru-telefoanele-mobile-smart/, accessed on 14.05.2020.

4 https://www.economica.net/elevii-de-gimnaziu-din-beijing-vor-purta-bra-ari-electronice-care-sa-trimita-avertizari-in-cazul-in-care-au-febra_184227.html, accessed on 14.07.2020.

5 https://adevarul.ro/international/in-lume/benjamin-netanyahu-vrea-cipuri-pielea-elevilor-expertii-securitate-cibernetica-opun-propunerii-1_5eb92e255163ec4271ab4810/index.html, accessed on 14.07.2020.

6 https://universul.net/tehnologii-infioratoare-invadeaza-europa-odata-cu-pandemia-analiza-bloomberg/,accessed on 14.07.2020.

7 *Ibidem.*

8 https://www.mediafax.ro/externe/politistii-cu-casti-de-supraveghere-ne-vor-identifica-si-ne-vor-lua-temperatura-din-mers-se-intampla-deja-in-china-dubai-si-italia-19144065, accessed on 14.07.2020.

9 https://www.mediafax.ro/externe/mossad-a-obtinut-10-milioane-de-masti-zeci-de-mii-de-teste-si-aparatura-medicala-din-surse-necunoscute-19031610, accessed on 18.07.2020.

10 https://www.jpost.com/israel-news/netanyahu-thanks-mossad-chief-for-purchasing-coronavirus-medical-gear-629161, accessed on 18.07.2020.

11 https://www.defenceromania.ro/serviciile-secrete-americane-i-israeliene-ar-fi-aflat-din-timp-de-coronavirus-us-army-neaga-raportul_602787.html, accessed on 18.07.2020.

12 The four great industrial revolutions (referred to in the literature−Industry 1.0 to Industry 4.0): mechanization, electrification, digitization, connectivity.

13 *Industry 5.0: Transforming the world into a SMART one.* The 5th Industrial Revolution will focus on the relationship between man and computer, the Internet of Things and smart grids.

14 Private armies, composed of mercenaries (usually former members of the special forces of the police, army, secret services) are a new way in which some governments want to achieve strategic goals without being officially involved in various conflicts; https://monitorulapararii.ro/fortele-hibride-mercenari-armate-private-1-21023, accessed on 18.07.2020.

15 https://www.capital.ro/vela-sa-fim-responsabili-sa-nu-credem-ca-virusul-nu-exista.html, accessed on 18.07.2020.

16 https://www.digi24.ro/stiri/actualitate/evenimente/un-elicopter-sovietic-care-zburase-clandestin-in-romania-a-fost-gasit-intamplator-la-patru-zile-de-la-prabusire-1128328, accessed on 18.07.2020.

17 https://www.eduapps.ro/aplicatii-educatie/classroom/, accessed on 18.07.2020.

18 https://www.wall-street.ro/articol/Turism/230215/10-orase-smart-din-lume-transformate-ireprosabil-de-tehnologie.html#gref, accessed on 18.07.2020.

19 https://economie.hotnews.ro/stiri-it-22098274-estonia-ajuns-atat-departe-digitalizarea-serviciilor-incat-poti-ajunge-doar-trei-ori-viata-semnezi-hartii-diversele-autoritati.htm, accessed on 18.07.2020.

20 https://monitorulapararii.ro/atacurile-cibernetice-permanent-in-umbra-conflictelor-din-orientul-mijlociu-1-28373, accessed on 18.07.2020.

21 *Ibidem*.

22 https://www.mediafax.ro/externe/atac-cibernetic-masiv-in-israel-exista-suspiciuni-ca-ar-fi-fost-lansat-de-iran-19163989, accessed on 18.07.2020.

23https://www.agerpres.ro/sci-tech/2016/02/12/atacul-cibernetic-ce-a-intrerupt-furnizarea-electricitatii-intr-o-regiune-a-ucrainei-a-fost-executat-din-rusia-17-06-10, accessed on 18.07.2020.

24 https://monitorulapararii.ro/pegasus-spionaj-prin-intermediul-telefonului-mobil-1-28477, accessed on 18.07.2020.

25 https://en.wikipedia.org/wiki/Pegasus_(spyware), accessed on 18.07.2020.

26 https://www.digi24.ro/stiri/sci-tech/lumea-digitala/spionii-israelieni-au-descoperit-ca-rusia-folosea-kaspersky-pentru-spionaj-809017, accessed on 18.07.2020.

27 https://universul.net/alerta-campanie-masiva-de-spionaj-prim-email-nume-de-mari-companii-folosite-ca-momeli/, accessed on 18.07.2020.

28 https://www.thelocal.de/20190927/germany-cracks-cyber-bunker-hosting-darknet-sites, accessed on 18.07.2020.

29 https://romanialibera.ro/international/justitia-belgiana-zadarniceste-propaganda-isis-prin-atacuri-cibernetice-815216

30 https://ro.wikipedia.org/wiki/Carlos_%C8%98acalul, accessed on 18.07.2020.

31 https://www.digi24.ro/stiri/externe/incident-de-natura-terorista-la-londra-un-barbat-a-injunghiat-mai-multe-persoane-pe-strada-1254062, accessed on 18.07.2020.

32 https://ro.wikipedia.org/wiki/Atentatul_de_la_Nisa_(2016), accessed on 18.07.2020.

33 https://stirileprotv.ro/stiri/international/autorul-atacului-de-la-pensacola-era-saudit-ce-a-publicat-acesta-pe-retele-sociale.html, accessed on 18.07.2020.

34 https://www.news.ro/externe/plan-atac-vizand-musulmani-dejucat-germania-tanar-arestat-dupa-s-laudat-internet-vrea-comita-atac-islamofob-cel-christchurch-zeelanda-arme-confiscate-domiciliul-suspectului-hildesheim-fisiere-192240520800202006121938490 2, accessed on 18.07.2020.

35 https://islamro.com/topic/618-daesh-public%C4%83-primul-num%C4%83r-al-unei-reviste-dedicate-securit%C4%83%C8%9Bii-cibernetice/?tab=comments#comment-975, accessed on 18.07.2020.

36 Titus Livius, *Istoria Romei de la întemeierea cetății – Enciclopedia înțelepciunii*, Editura Rossa, p. 108.

37 https://monitorulapararii.ro/epoca-razboaielor-dronelor-aeriene-s-a-instalat-definitiv-1-31794, accessed on 18.07.2020.

38 https://www.hotnews.ro/stiri-international-22877928-haos-aeroportul-gatwick-inchis-peste-17-ore-din-cauza-unor-drone-neidentificate.htm, accessed on 18.07.2020.

39 https://www.mediafax.ro/externe/atacuri-cu-drone-in-arabia-saudita-doua-instalatii-petroliere-sunt-afectate-de-incendii-masive-insurgentii-huthi-din-yemen-revendica-atentatele-video-18398347, accessed on 18.07.2020.

40 https://www.digi24.ro/stiri/externe/autoritatile-ii-ur maresc-cu-drona-pe-chinezi-si-ii-someaza-sa-poarte-masca-bunico-nu-te-mai-holba-du-te-si-spala-te-pe-maini-1254243, accessed on 21.07.2020.

41 On 26 June 2018, the Council adopted new proportionate and risk-based rules that will allow the EU aviation sector to grow and become more competitive. The new rules also apply to the registration threshold for drone operators: they should be registered if their drones can transfer a kinetic energy of more than 80 joules to the impact with a person, https://www.consilium.europa.eu/ro/policies/drones/, accessed on 21.07.2020.

42 http://legislatie.just.ro/Public/DetaliiDocument/223897, accessed on 21.07.2020.

43 https://www.g4media.ro/marea-britanie-acuza-rusia-ca-a-incercat-sa-se-amestece-in-alegerile-parlamentare-din-2019-achizitionand-ilegal-si-difuzand-online-documente-sensibile-referitoare-la-acordul-de-liber-schimb-cu-statel. html, accessed on 21.07.2020.

44 https://www.stiripesurse.ro/democratiile-occidentale-o-resursa-imensa-pentru-rusia-kremlinul-a-incercat-sa-intervina-si-in-referendumul-pentru-independenta-scotiei_1487574.html, accessed on 21.07.2020.

45 https://www.stiripesurse.ro/avertismentul-nsa-cu-privire-la-alegerile-americane-vom-actiona-atunci-cand-vom-vedea-ca-adversarii-nostri-incearca-sa-se-amestece_1487511.html, accessed on 21.07.2020.

https://www.stiripesurse.ro/serviciu-secret-detoneaza-bomba-china-rusia-si-iranul-incearca-sa-influenteze-rezultatul-alegerilor-din-sua_1488962.html, accessed on 21.07.2020.

46 https://www.euractiv.ro/extern/departamentul-justitiei-a-deschis-o-ancheta-penala-in-cazul-investigatiei-privind-ingerintele-ruse-16368, accessed on 21.07.2020.

4 https://www.stiripesurse.ro/democratiile-occidentale-o-resursa-imensa-pentru-rusia-kremlinul-a-incercat-sa-intervina-si-in-referendumul-pentru-independenta-scotiei_1487574.html, accessed on 21.07.2020.

48 https://www.caleaeuropeana.ro/duma-de-stat-a-rusiei-infiinteaza-o-comisie-de-ancheta-a-ingerintelor-externe-in-favoarea-protestelor-de-la-moscova/, accessed on 21.07.2020.

49 http://www.europarl.europa.eu/doceo/document/B-9-2019-0108_RO.html, accessed on 21.07.2020.

50 August 5, 2020, US Secretary of State: "The United States offers a reward of up to $ 10 million for information that allows the identification or location of any person who, acting on the orders or under the control of a foreign government, intervenes in the US elections", https://www.g4media.ro/mike-pompeo-sua-ofera-o-recompensa-de-10-milioane-de-dolari-pentru-arestarea-oricarei-persoane-care-intervine-in-alegerile-din-noiembrie.html, accessed on 21.07.2020.

51 https://www.digi24.ro/stiri/externe/ue/cum-a-influentat-cambridge-analytica-referendumul-privind-brexit-902773, accessed on 21.07.2020.

52 *Ibidem*.

53 https://www.imdb.com/title/tt8425058/, accessed on 21.07.2020.

54 https://ziaristii.com/au-prins-spionajul-rus-implicat-haosul-din-catalunya-si-destabilizarea-europei-serviciile-secrete-din-ue-confirma-mana-rusiei-actiuni-grave-pe-continent/, accessed on 21.07.2020.

55 Cognitive fluency and attitudinal change mechanisms, Andrei Holman, *Social Psychology*, Issue 10 / 2002, pp. 90-107.

56 http://www.viitorul.org/files/4392299_md_studiu_informa.pdf, accessed on 21.07.2020.

57 http://www.ziare.com/europa/moldova/alegeri-la-chisinau-fara-stat-de-drept-libertate-de-exprimare-si-

deschidere-catre-lume-nu-vom-avea-nici-integrare-europeana-nici-unire-cu-romania-interviu-1551002, accessed on 21.07.2020.

58 https://www.digi24.ro/stiri/externe/ue/document-rusia-desfasoara-o-semnificativa-campanie-de-dezinformare-in-ue-cu-privire-la-coronavirus-1277347, accessed on 21.07.2020.

59 https://www.state.gov/briefing-with-special-envoy-lea-gabrielle-global-engagement-center-on-disinformation-and-propaganda-related-to-covid-19/, accessed on 21.07.2020.

60 https://www.nytimes.com/2020/04/10/technology/coronavirus-5g-uk.html, accessed on 21.07.2020.

61 http://m.ziare.com/media/finlanda-incepe-lupta-cu-fake-news-din-scoala-primara-si-da-rezultate-1595955, accessed on 21.07.2020.

62 http://m.ziare.com/media/finlanda-incepe-lupta-cu-fake-news-din-scoala-primara-si-da-rezultate-1595955, accessed on 21.07.2020.

63 Industry 5.0 transforming the world into a Smart one. The 5th Industrial Revolution will focus on the relationship between man and machine.

64 https://www.ft.com/content/8b48f460-50af-11e9-9c76-bf4a0ce37d49, accessed on 21.07.2020.

65 https://www.mediafax.ro/economic/avertismentul-sua-in-legatura-cu-huawei-si-tehnologia-5g-ei-vor-doar-sa-fure-secrete-de-stat-18678540, accessed on 21.07.2020.

66 https://www.mediafax.ro/life-inedit/china-introduce-recunoasterea-faciala-obligatorie-pentru-utilizatorii-de-telefoane-mobile-18637109, accessed on 21.07.2020.

67 Fictional character, illustrating dictatorial, totalitarian tendencies, https://www.britannica.com/topic/Big-Brother-fictional-character, accessed on 21.07.2020.

68 George Orwell, *1984 Nineteen Eighty-Four*, Penguin Books Ltd, 1991.

69 https://libra.org/en-US/, accessed on 21.07.2020.

70 https://monitorulapararii.ro/inteligenta-artificiala-in-intelligence-si-nu-numai-1-28414, accessed on 21.07.2020.

71 https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1701&context=jss, accessed on 21.07.2020.

72 https://monitorulapararii.ro/razboaiele-din-siria-si-afganistan-vor-fi-privatizate-1-11282, accessed on 21.07.2020.

73 https://www.digi24.ro/stiri/externe/mapamond/raport-onu-cum-lupta-armata-privata-a-lui-putin-in-libia-de-partea-fortelor-rebele-1303476, accessed on 21.07.2020.

74 https://www.g4media.ro/mercenarii-rusiei-ce-sunt-si-cum-actioneaza-micile-armate-private-comandate-de-moscova-cazul-wagner-sau-cum-a-decazut-cea-mai-mare-companie-rusa-de-securitate.html, accessed on 21.07.2020.

REFERENCES

Buzan Barry, *People State and Fears*, Brighton, Harvester Press, 1983.

Fox C. Amos, *Conflict and the Need for a Theory of Proxy Warfare*, https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1701&context=jss

Fridman Ofer, Kabernik Vitaly, Pearce C. James, *Hybrid Conflicts and Information Warfare: New Labels, Old Politics*, 1st Edition, 2018.

Haacke Jürgen, *Asean's Diplomatic and Security Culture. Origins, development and prospects*, Antony Rowe Ltd., Chippenham, Wiltshire, Great Britain, 2003.

Hoffman G. Frank, *Conflict in the 21th Century: the Rise of the Hybrid Wars*, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Holman Andrei, "Cognitive fluency and attitudinal change mechanisms", *Social Psychology (Psihologia socială)*, Issue 10/2002, https://www.ceeol.com

Iancu N., Fortuna A., Barna C., Teodor M., *Countering Hybrid Threats: Lessons Learned from Ukraine* (NATO Science for Peace and Security), 2016.

Micossi Stefano, Tosato Gian Luigi, *The European Union in the 21st Century. Perspectives from the Lisbon Treaty*, Center for European Policy Studies, Brussels, 2009.

Orenstein A. Mitchell, *The Lands in Between: Russia vs. the West and the New Politics of Hybrid War*, 1st Edition, 2019.

Răducanu Gabriel, Anastasiei Traian, *Challenges To Global Security*, http://www.afahc.ro/ro/revista/2017_1/17-GabrielRaducanu,TraianAnastasiei.pdf

Dr. Russell W. Glenn, *Thoughts on "Hybrid" Conflict"*, https://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict

Stowell Joshua, *What is Hybrid Warfare?*, https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/

Titus Livius, *Istoria Romei de la întemeierea cetății – Enciclopedia înțelepciunii*, Editura Roossa, 2013, https://www.newmoney.ro/

http://www.rador.ro/

https://www.economica.net/

https://adevarul.ro/

https://universul.net/

https://www.defenceromania.ro

https://www.capital.ro/

https://www.eduapps.ro/

https://www.wall-street.ro/

https://www.agerpres.ro/
https://en.wikipedia.org/
https://www.thelocal.de/
https://romanialibera.ro/
https://www.news.ro/
https://islamro.com/
https://monitorulapararii.ro/
https://www.hotnews.ro/
https://www.mediafax.ro/
https://www.digi24.ro/
https://www.consilium.europa.eu/
http://legislatie.just.ro/
https://www.g4media.ro/
https://www.stiripesurse.ro/
https://www.euractiv.ro/
https://www.caleaeuropeana.ro/
http://www.europarl.europa.eu/
https://www.imdb.com/
https://ziaristii.com/
https://www.state.gov/
https://www.nytimes.com/
https://www.ft.com/
https://libra.org/en-US/