

Anul XII nr. 3/2020

INFOSFERA

Revistă de studii de securitate și informații pentru apărare

Publicație indexată în bazele de date internaționale EBSCO și CEEOL

**Revistă cu prestigiu științific recunoscut de Consiliul Național de Atestare
a Titlurilor, Diplomelor și Certificatelor Universitare (CNATDCU)**

Direcția Generală de Informații a Apărării

CUPRINS

<i>Romania – A soft power leader in Eastern Europe and the Black Sea Region.....</i>	<i>3</i>
David H. CARSTENS	
<i>Identitatea națională – între naționalism și multiculturalism.....</i>	<i>14</i>
Cristian DOBRE	
<i>Limitele aranjamentelor post-conflict. Feudalizarea sectară și implozia sistemului politic libanez.....</i>	<i>23</i>
Iulian CHIFU	
<i>Coordonatele războiului de generația a cincea.....</i>	<i>33</i>
Daniel COCOLICI Sorinel POPESCU	
<i>Forțele aeriene, factor de descurajare în procesul de escaladare a crizelor</i>	<i>41</i>
Vasile-Cristian ONESIMIUC	
<i>Impactul crizei medicale generate de pandemia de COVID-19 asupra actorilor statali.....</i>	<i>49</i>
Alba Iulia Catrinel POPESCU	
<i>Efectele pandemiei de COVID - 19 în spațiul cibernetic.....</i>	<i>58</i>
Constantin NILĂ Marius PREDA Cornel ARGINT	
<i>Cauzele manipulării informațiilor de la nivelul individului</i>	<i>64</i>
Ilie CRISTIAN	
<i>Provocări asociate surselor deschise în activitatea de intelligence</i>	<i>71</i>
Rareș TĂBLEȚ	
<i>Utilizarea rețelelor sociale. Riscuri și vulnerabilități la adresa personalului Ministerului Apărării Naționale</i>	<i>78</i>
Răzvan ZMĂDU	
<i>Acțiuni ale serviciilor secrete țariste în România, în epoca modernă</i>	<i>89</i>
Ioan-Codruț LUCINESCU	

ROMANIA – A SOFT POWER LEADER IN EASTERN EUROPE AND THE BLACK SEA REGION

*David H. CARSTENS**

Abstract

Romania is a committed North Atlantic Treaty Organization (NATO) ally and the cornerstone of Black Sea security. Despite Romania's demonstrated NATO contributions, perhaps we are underestimating the country's capabilities and potential when it comes to deterrence. What Romania proved most during the COVID-19 pandemic response was that it could embrace the values of leadership, contribution and positive influence by rapidly extending medical aid to countries such as Italy, the Republic of Moldova and even the United States while simultaneously responding to its own crises at home. The Romanian military was the ultimate tool in this form of soft-power projection: agile enough to rapidly deploy medical aid, flexible enough to manage traditional civil institutions such as local/regional hospitals when called upon by the government to do so and innovative enough to re-tool parts of its defense industry to produce COVID-19 related equipment on a moment's notice. These are remarkable achievements that can be used to influence partners and neighbors in Eastern Europe and the Black Sea region. We should re-evaluate Romania's increased potential to NATO, the European Union (EU) and bilateral relations with the United States, specifically in the area of soft power projection.

Keywords: *Black Sea security, Romania, COVID-19, soft power leader, hub vaccine, lessons learned.*

Romania: A Valued and Extremely Capable NATO Ally

Romania is a committed NATO ally and the cornerstone of Black Sea security. It is the sixth largest contributor of forces to NATO's RESOLUTE SUPPORT mission in Afghanistan, among the 38 contributing nations. Romania is on a glide path to spend 2% of gross domestic product (GDP) on defense spending: they came close in 2019, spending an estimated 1.96% of GDP. They are pushing forward with key investments in air defense (Patriot missiles), rocket launched artillery (High Mobility Artillery Rocket Systems/HIMARS), F16s and maritime early warning equipment, all of which will provide a much-needed boost to NATO's Eastern flank in the face of increasing Russian aggression. In late April 2020, with the COVID-19 crisis

rapidly unfolding, Romania's Chief of Defense Daniel Petrescu secured parliamentary approval to move forward with all defense procurement projects: yet another sign of Romania's long-term commitment and contributions to Black Sea security.

Romania continues to display its military leadership within the NATO framework by hosting the (soon-to-be) Multi-National Corps Southeast, some of the largest multi-national exercises in Europe (SABER GUARDIAN and upcoming DEFENDER 21), and the Joint National Training Center, Cincu: a world-class, digitally robust training center for combined military operations up to brigade-level.

Romania also serves as a formidable power projection platform for NATO with a sprawling logistics hub at Mihail Kogălniceanu Air Base

* *Colonel (retired), U.S. Army.*

(MKAB), a short 25-minute drive to the port of Constanta: Europe's 13th largest port and the largest on the Black Sea. The base is also strategically located near the mouth of the Danube river, an underutilized logistical lifeline which snakes back into the heart of Europe. Another power projection capability that has not been fully realized is Cămpia Turzii Air Base (CTAB). CTAB is an ideal base for fighter aircraft and strategic UAVs given its remote location, flying conditions, distance to potential targets, and all-weather airfield clearing capability to support launch/recovery operations. Romania's Ministry of National Defense is investing heavily in both locations: more than doubling the land holdings of each and investing millions of Euro's in infrastructure, security, and other improvements for expanded operations.

Despite Romania's demonstrated NATO contributions, perhaps we are underestimating the country's capabilities and potential when it comes to deterrence and should re-evaluate Romania's role in NATO, the EU and bilateral relations with the U.S., specifically in the area of soft power projection.

Romanian Military: Instrument of Soft Power during Pandemic

American political scientist Joseph Nye coined the term "soft power" in the late 1980s. He defined it as the ability of a country to persuade others to do what it wants without force or coercion. Nye went on to argue that successful states need both hard and soft power: "the ability to coerce others as well as the ability to shape their long-term attitudes and preferences"¹. Soft power is difficult to quantify. "If a state can make its power seem legitimate in the eyes of others, it will encounter less resistance to its wishes". That is, Nye argued, "if its culture and ideology are attractive, others will more willingly follow"².

For Nye, the basis of U.S. soft power was liberal democratic politics, free market economics, and fundamental values such as human rights.³ For Romania, the basis of soft power could be the same democratic politics combined with building medical and first responder capacity and institutions, and values such as leadership, contribution, and positive influence. In this context, Romania is poised to become a soft power leader in Eastern Europe



Romanian medical personnel arriving in Italy as part of "resc EU" humanitarian assistance



***20 Romanian military trucks with medical aid bound
for the Republic of Moldova on 6 May 2020.***

Photo Source: Inquam Photos/Octav Ganea, Romania-Insider.com (6 May 2020)

and the Black Sea region and NATO, the EU and the U.S. must rise now to reinforce this incredible potential.

During the COVID-19 pandemic, doctors, respirators and personal protective equipment, not soldiers, tanks and aircraft, have taken center stage in the fight to maintain national security. Under these unprecedented conditions, the Romanian military proved itself capable of adapting rapidly and setting the conditions for increased soft power projection throughout Eastern Europe and the Black Sea region. Areas of recently demonstrated tools of soft power include:

Rapid Deployment of Emergency Medical Personnel, Equipment and Infrastructure: During the early stages of the pandemic with Romania still very much struggling to contain its own COVID-19 outbreak, the Government of Romania stepped up as a leader in the first “rescEU” mission, carried out as a part of the European Union’s Civil Protection Mechanism. Romania self-deployed both medical supplies and a team of doctors/nurses to Italy, on board a Romanian Air Force C-27 aircraft⁴. The team, made up of both Romanian volunteers and

military medical personnel, worked in Lombardy Italy hospitals for 18 days, from 7-24 April 2020. The deployment was highly regarded by European leaders and touted as “EU solidarity in action”⁵.

On 20 May 2020, the Romanian Parliament approved participation of the Romanian military in humanitarian assistance missions in the Republic of Moldova and the U.S. The U.S. support mission departed 25 May 2020 and was comprised of 15 personnel: five military doctors, five military nurses, and five chemical/biological/nuclear specialized officers. The Romanian medical team provided two-weeks of support in several Alabama cities in partnership with the Alabama National Guard⁶.

Romania also completed two medical assistance missions to the Republic of Moldova: one in April 2020, involving the deployment of 42 doctors and nurses to the Republic of Moldova’s three largest cities and another one on 6 May 2020, involving the distribution of medical supplies and other COVID-19 related aid. The latter support package was self-deployed by 20 Romanian military trucks which



Inside view of the Romanian military hospital installed at the Ana Aslan Institute in Otopeni¹¹.

transported 500,000 FFP2 protective masks, 25,000 bio-resistant coveralls, 5,000 face masks, 5,000 protective glasses, 200,000 gloves, 2,800 medicine boxes, ten isolation stretchers, and approximately 80,000 liters of sanitary alcohol⁷. Total cost of the aid package was estimated at RON 16.5 million (approximately \$3.7 million USD), allocated from Romania's Reserve Fund.

Self-deploying doctors and nurses are not the only thing that Romania can do in response to a medical emergency. The Romanian Ministry of National Defense established a ROLE 2 field hospital on the north side of Bucharest in the early stages of the pandemic. The field hospital consisted of medical tents and containers and included functions such as a triage zone, laboratory, radiology section, sterilization zone and a decontamination area. A similar military hospital was established in Timisoara, Romania.

The construction and set-up were completed in 5-days and the hospital was declared operational on 28 March 2020. The same ROLE 2 military hospital was deployed in 2015 when it was prepared to treat possible Ebola infection cases. It was also used in NATO military exercises in 2019, including VIGOROUS WARRIOR: the largest medical military exercise ever organized by NATO and hosted by Romania⁸.

Emergency and Crisis Management: On 24 March 2020, the Romanian Ministry of National Defense was called in to enforce a series of military ordinances which limited movement inside localities and across the country and maintained order to help stop the spread of COVID-19⁹. This was done in close cooperation with the Ministry of Interior Affairs. Romanian Land Forces vehicles were seen on the streets alongside the Romanian police and gendarmerie throughout the pandemic.

Additionally, the Government of Romania put the Romanian army in charge of three hospitals during the pandemic. One of these was in the northern town of Suceava, Romania's initial epicenter for COVID-19. The army was called in to bring discipline and process rigor to what was a situation deteriorating in both health and discipline¹⁰.

Military Research and Development and Rapid Acquisition: In response to COVID-19, the Romanian Ministry of National Defense quickly pushed through several COVID-19 related developments. The Military Technical Academy "Ferdinand I" in Bucharest, a polytechnic university of the Ministry of National Defense, developed a mechanical ventilator to be used

by hospitals treating coronavirus patients. The Military Academy designed and patented the ventilator in record time and a manufacturer of equipment and solutions used in the defense industry developed the product into the prototype phase¹².

At the same time, Romanian army researchers quickly designed and patented an isolation stretcher and production was approved immediately thereafter. The new equipment ensures the temporary isolation and safe transport of people suspected or confirmed as being infected with COVID-19. It has a filtered air ventilation system and meets all safety standards to avoid contamination during transportation¹³.

Romanian military working with police to enforce COVID lockdown.

Romanian military contractors rapidly retooled to produce COVID-19 related equipment. Companies Pro-Optica and Întreprinderea Optică Română (IOR) partnered to develop and manufacture a thermal scanner that allows the precise and rapid determination of body temperatures. The scanner can be used in areas with a high influx of people, such as airports, subways, border crossing points, triage points of

hospitals, or in public institutions, to reduce fever assessment times¹⁴.

Romanian Military: Post COVID-19 Lessons Learned

The Ministry of National Defense will no doubt continue to self-evaluate its performance in a series of post-COVID-19 after action reviews. The results remain to be seen but there's one thing for certain: the Ministry of National Defense must maintain a close relationship with the inter-agency in regards to emergency management and crisis response. This could result in the establishment of emergency management cells inside military headquarters, compatible communications networks, and the exchange of liaison officer (LNOs) between the Romanian military and their inter-agency partners.

Ultimately, the Romanian military should consider development of a program similar to the U.S. Army Protection Program (APP): the program of record which enables the execution of Army missions in all threats and hazards environments and by integrating, coordinating, synchronizing, and effectively prioritizing efforts and resources¹⁵. The APP addresses



Romanian military working with police to enforce COVID lockdown

the non-warfighting functional elements of: antiterrorism, computer network defense, continuity of operations, critical Infrastructure risk management, emergency management, fire and emergency services, health protection, high-risk personnel, information assurance, law enforcement, operations security, and physical security; and the enabling functions of: intelligence, counterintelligence, and security engineering services¹⁶. At the division and corps levels, the G34 Protect staff directorate informs the Commander on all threats and hazards within his or her area of responsibility and ensures these threats are accounted for in the operational scheme of maneuver. Equally important, the G34 provides a much-needed link between U.S. Army commands at the division level and above and organizations like the Federal Emergency Management Agency (FEMA).

Romania's European and Trans-Atlantic Soft Power Potential

Reliance on Chinese-made pharmaceuticals is a risk to EU security as well as U.S. interests, which include U.S. Service Members forward stationed in and forward deployed to Europe: a fact made even clearer in the current COVID-19 plagued world. Perhaps the greatest soft power potential that Romania possesses is the ability to produce vaccines at a large scale to meet both national, European and even trans-Atlantic demands.

The Institute Cantacuzino was established in 1921. The purpose of the institute was to immunize Romania's population against epidemics and pandemics. In its heyday, the Cantacuzino Institute was the largest of its kind in southeastern Europe relative to volume of serum and vaccine production. The Institute's experts were also in charge of medical diagnosis, research, public health and education. As a result of the Institute's activity, smallpox was eradicated in Romania and the Romanian population was protected from tuberculosis, tetanus, diphtheria, cholera and other infectious diseases. At the peak of its production, the Institute produced almost 400 serums, vaccines and drugs and offered

immunizations to millions of Romanians during its 70 years of existence. The Institute was part of the select global circuit of Pasteur Institutes in Paris, France and as such, Pasteur Institute training sessions and research were conducted in Romania.

Institute Cantacuzino stopped making vaccines in 2014 and requires investment by Romania, the EU and International partners. The Romanian Ministry of European Funds is working on a non-refundable 150 million Euro project to modernize the Institute and restart vaccine production tailored to specific requirements necessary to meet current and future epidemics and pandemics.

Dr. Alexandru Rafila is currently Chief, National Institute for Infectious Diseases in Bucharest, Romania. His expertise is fully recognized by World Health Organization (WHO), NATO and the European Commission and he is the leading expert in the fight against COVID-19 in Romania. Dr. Rafila believes the Institute could restart production of two vaccines (flu and BCG) as well as: "...more, complex vaccines like the Institute used to produce (measles, diphtheria, tetanus vaccines and others) could be produced in partnership with a big vaccine producer. The Institute could produce a large variety of vaccines that are part of the national vaccination programs in Romania, other EU member states and non-EU countries". The Cantacuzino Institute was placed under the Romanian Ministry for National Defense in 2017 and is considered of national security importance.

A fully operational vaccine production facility in Romania would not only provide long term security to Romania, but it could provide a regional vaccine capability as well. Given the strategic partnership between the U.S. and Romania, a rebuilt pharmaceutical industry in Romania could also provide an alternative source to Chinese-made pharmaceuticals, of which there are growing security and safety concerns. About 80 percent of the active pharmaceutical ingredients used to make drugs in the United States are said to come from China¹⁷. In 2008, at least 81 U.S. deaths were linked to the contamination of

an imported Chinese raw ingredient used to make heparin, a blood thinning drug. In 2018, one of China's largest domestic vaccine makers sold 250K substandard doses of vaccine for diphtheria, tetanus and whooping cough¹⁸. The concern over U.S. dependency on Chinese pharmaceuticals is real and growing and cannot be underestimated.

The Black Sea Region: Romania in a Dangerous Neighborhood

Romanian military strategists and intelligence professionals often remark that while Russia *threatens* in the Baltics, they *act* in the Black Sea region. History has proven the Romanian's assessments correct time and time again. One need only to point to Russia's 2008 illegal occupation of Georgia's Abkhazia and South Ossetia territories, Russian-backed breakaway state Transnistria, Russia's 2014 invasion and annexation of Crimea, continued hostilities in eastern Ukraine, and most recently, the 2018 seizure of Ukrainian naval ships in the Sea of Azov as stark reminders of Russia's continuous hostile actions in the Black Sea region.

More concerning is that the COVID-19 pandemic has brought severe economic strain to the global economies, most notably in Russia where decreased oil demand and an oil production war with Saudi Arabia contributed to a cataclysmic drop in the price of oil. In the past, Russia has used periods of economic crisis to focus its disenfranchised population on exaggerated "external threats". In 1999, during a period of economic crisis, Russia launched the second Chechen war; during the 2008 economic crisis, Russia occupied territories in Georgia; and during the 2014 economic drop, the Crimea invasion. It would not be surprising for Russia to act in a similarly aggressive manner in the Black Sea region during what will surely become the post COVID-19 economic depression.

China is also no stranger to the Black Sea, fully invested in building a modern silk road to Europe (also known as, "One Belt, One Road" Initiative). China is cautious not to antagonize Russia in an area of traditional Russian dominance rife with geo-political sensitivities²⁰. China's influence is less military and more economic

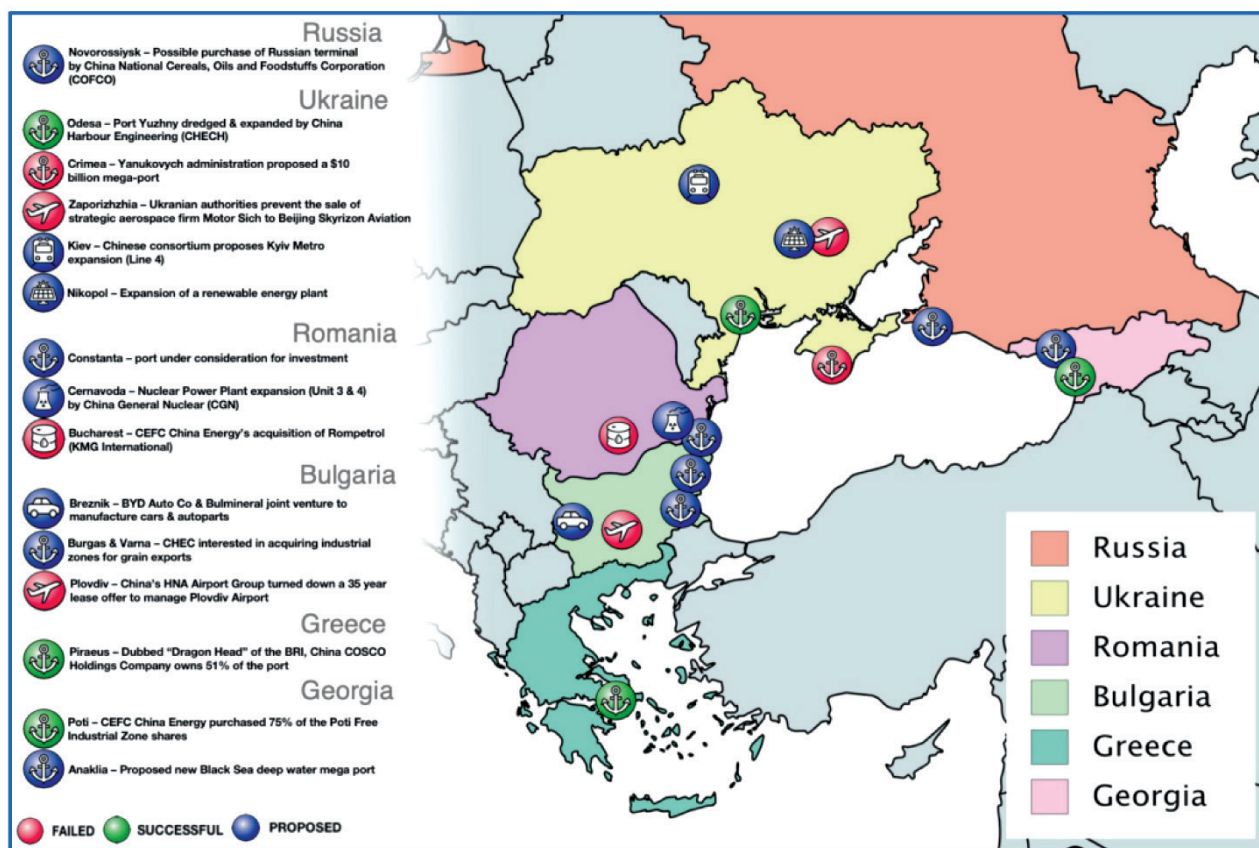


Figure 1: Chinese economic investment as a vehicle for political influence¹⁹.

based, with the intent of acquiring strategic industrial platforms and offering loans for large development projects²¹. In Romania, Chinese influence can be plainly seen in brazen attempts to help Romania re-tool its nuclear power facility at Cernavodă and continued aggressive push for Huawei entry into Romania's 5G market. While Romania successfully rebuffed Chinese efforts to partner in nuclear energy, it remains to be seen if other Chinese efforts in Romania will be similarly thwarted.

Despite the fact that Chinese-backed projects often fail or come with China-friendly strings attached, they continue to be an attractive alternative when no other (European or U.S.) funding is available. In Romania for example, the Bank of China recently had talks with the Government of Romania about funding for the long-sought-after Comarnic to Brasov highway project. Unless viable alternatives are found, this project will be built by a Chinese company with financing secured by the Bank of China²².

Much of the Russian and Chinese malign influence in Eastern Europe and the Black Sea region is subtler, relying on traditional propaganda platforms which have exploded in response to the pandemic. While governments have been sheltering in a global lockdown, Russia and China are working in unison to spread disinformation, downplay U.S. (and EU) COVID-19 aid efforts and exaggerate Russian and Chinese aid efforts.

During the COVID-19 crisis, the Chinese embassy in France accused French politicians and medical workers of failing to assist their citizens. China's Embassy in Italy promoted Beijing's capability and willingness to provide support to meet European need²³. Closer to Romania, Russia continued this pattern of Europe bashing in the Republic of Moldova: manipulating the current pro-Russian government to minimize Romanian COVID-19 aid convoys and medical assistance and over-state trivial efforts by Russia to do the same. The Republic of Moldova's Russian-backed government went so far as to set up an elaborate scheme to extend bribes to the 42 Romanian doctors and nurses who arrived at the border between the two countries in early May.

While the money was given back to the corrupt Republic of Moldova official who gave it to them in the first place, it serves as a disturbing reminder to the lengths Russia (and China) will go to press their malign influence agenda.

Romania: Near Term Potential Soft Power Objectives

Not only does Romania have effective instruments to exert its soft power influence as demonstrated repeatedly during the COVID-19 crisis, but Romania is geographically positioned in the "dangerous neighborhood" where Romanian efforts can counter Russian and Chinese influence. Here are some specific examples of where NATO and the EU can leverage Romania's soft power potential:

(1) Build a more effective image of the EU in the Republic of Moldova to counter Russian influence. The Republic of Moldova is floundering, descending rapidly into the arms of Russia and the EU (and U.S.) influence is losing the battle on all fronts. Moldovan President Igor Dodon is unabashed in his love for all things Moscow and EU influence in the Republic of Moldova parliament is weak at best. As diplomatic efforts continue, Romania can serve as a platform for continued soft power influence on its neighbor.

Multi-lateral military-to-military engagements with the Republic of Moldova, focused on medical aid and emergency management, could best show the EU flag when it's needed most in a manner that is non-confrontational to Moscow. Aerial MEDEVAC, the establishment of field hospitals and other visual medically focused boots-on-the-ground exercises would be an excellent tool of influence. The U.S. could assist with logistics: strategic air transport from Ramstein to Mihail Kogălniceanu to Chișinău, as a means of further demonstrating its own brand of power projection.

(2) Partner with Ukraine and Georgia to Build Institutions. Both Ukraine and Georgia have had good relationships with Romania in recent years. One thing is for certain: all three are linked by their concern over continued Russian aggression. Unfortunately, Ukraine and Georgia

have Soviet-era style acquisition processes which could use an infusion of good (Western) ideas from a friendly neighbor. Romania should reach out with its growing military industrial and research and development institutions to help both countries refine their advance acquisition processes, focusing on the lessons learned producing COVID-19 protective equipment.

(3) Lead NATO Post COVID-19 After Action Review Processes and Participate in Doctrine Development: The Romanian military has lots of lessons learned to share with NATO and the EU. In leading the process, Romania can show to NATO and the EU that they are a knowledgeable and legitimate player when it comes to international crisis response and emergency management. A venue to share these lessons learned NATO-wide could be the NATO Center of Excellence for Crisis Management and Emergency Response (CMDR COE). The CMDR COE is a multi-national NATO military organization sponsored by Greece, Poland and Bulgaria with the Center located in Sophia, Bulgaria²⁴.

(4) Host an Annually Recurring Emergency Management Multi-National Exercise: NATO and the EU should adapt to the lessons learned from the current pandemic by focusing doctrine development and exercises on emergency management and crisis response. Since Romania is already an experienced leader in hosting multi-national exercises, why not build upon this existing framework by conducting the first such emergency management exercise in Romania? The scenario of such an exercise should drive a NATO/EU response to a national or regional emergency: such as pandemic outbreak. The exercise should focus on rapid deployment of first responders, medical logistics, collaboration with the inter-agency, and what the military calls, “mission command”. Equal to the resulting readiness increase that such an exercise would bring is the counter-malign influence message it would send to Moscow and Beijing: that NATO is ready, willing and able to assist allies and partners in any contingency.

Investment in Romania to Capitalize on Soft Power Potential:

Develop Romania into a Regional Vaccine Hub: As previously stated, Romania’s potential to re-start vaccine production through the Institute Cantacuzino, is likely the single-most powerful generator of soft power influence in the region. An infusion of EU funds and a long-term partnership with a pharmaceutical leader could awaken this vaccine sleeping giant and ensure that Romania, Europe and trans-Atlantic partners can remain independent of Chinese pharmaceutical markets for the foreseeable future. A restart of the Institute would also allow Romania to focus on research and development to fend off the next pandemic: a major national security win.

Expand and Leverage the Network: A lesson learned from the pandemic is a reliance on virtual environments for everything from business to teaching. The Government of Romania and the military should take the same approach when it comes to emergency management. Growth in this area is stunted by Romania’s poor internet connectivity in the rural areas. In a 2017 report by the European Commission on Europe’s Digital Progress, Romania was ranked last in the EU’s Digital Economy and Society Index (DESI)²⁵. The DESI’s five dimensions include connectivity (broadband speed and prices), human capital (skills at using the internet), use of the internet (for content, transactions, and communications), integration of digital technology, and digital public services.²⁶ Increasing internet connectivity in Romania with emphasis on the rural areas (which lack all basic digital services), will not only allow for a viable emergency management network, but it could also provide the backbone for telehealth resources: an absolute necessity during periods of limited mobility. Using traditional allies to form new partnerships – like engagement with the U.S. Landstuhl Regional Medical Center, Europe’s largest military hospital with a vast telehealth network – could bring increased technical capability when launching first responders across the region.

A revitalized network and expanded Internet can also be leveraged for distance learning: a major capability gap in Romania's rural areas. More educated Romanians in these hard-hit rural areas could become less susceptible to Russian and Chinese manufactured fake news and malign influence: a much-needed benefit resulting from this investment.

Conclusion

Romania is already showing what it takes to become a regional leader in the area of soft power. The current government is focused more on rule of law and upholding the principles of liberal democratic politics than at any other time in the country's recent past. What Romania proved most during the pandemic response is that it could embrace the values of leadership, contribution and positive influence by rapidly extending medical aid to countries such as Italy, the Republic of Moldova and even the United States while simultaneously responding to its own

crises at home. The Romanian military was the ultimate tool in this soft-power projection, agile enough to rapidly deploy medical aid, flexible enough to manage traditional civil institutions such as local/regional hospitals when called upon by the government to do so and innovative enough to re-tool parts of its defense industry to produce COVID-19 related equipment on a moment's notice. These are remarkable achievements that can be used to influence partners and neighbors in Eastern Europe and the Black Sea region. Moreover, Romania has the potential to become a pharmaceutical leader in Europe, extending its soft power influence even further by helping allies and partners defend themselves from the invisible pandemic threats of the future while simultaneously blocking inferior and potentially life threatening Chinese pharmaceutical products.

It's time for NATO, the EU and the U.S. to acknowledge and reinforce Romania's soft power potential.

¹ Joseph Nye Jr., "Soft Power: The Means to Success in World Politics," quoted in G. John Ikenberry's capsule review in *Foreign Affairs* (May/June 2004): <https://www.foreignaffairs.com/reviews/capsule-review/2004-05-01/soft-power-means-success-world-politics> (accessed 1 Aug 2020).

² Eric Li, "The Rise and Fall of Soft Power," *Foreign Policy* (20 Aug 2018): <https://foreignpolicy.com/2018/08/20/the-rise-and-fall-of-soft-power/> (accessed 1 Aug 2020).

³ Idem.

⁴ "Romanian Doctors and Nurses Will Work in Italy to Help Combat the COVID-19 Outbreak," Government of Romania press release (7 Apr 2020): <https://gov.ro/en/news/romanian-doctors-and-nurses-will-work-in-italy-to-help-combat-the-covid-19-outbreak> (accessed 1 Aug 2020).

⁵ "Coronavirus: EU Medical Teams Deployed to Italy," European Commission press release (7 Apr 2020): https://ec.europa.eu/commission/presscorner/detail/en/ip_20_613 (accessed 1 Aug 2020).

⁶ "SPP Spirit Spurs Romania to Help Alabama Fight COVID-19," United States Army (26 May 2020): https://www.army.mil/article/235925/spp_spirit_spurs_romania_to_help_alabama_fight_covid_19 (accessed 1 Aug 2020)

⁷ "Coronavirus Pandemic: Romania Sends Medical Equipment to Moldova," Romania-Insider.com (6 May 2020): <https://www.romania-insider.com/romania-medical-equipment-moldova> (accessed 1 Aug 2020).

⁸ "Coronavirus in Romania: Mobile Military Hospital Installed Near Bucharest Becomes Operational," Romania-Insider.com (30 Mar 2020): <https://www.romania-insider.com/coronavirus-military-hospital-bucharest> (accessed 1 Aug 2020).

⁹ "Coronavirus: Romania Moves to Full Virus Lockdown Enforced by Army," Deccan Herald (24 Mar 2020): <https://www.deccanherald.com/international/world-news-politics/coronavirus-romania-moves-to-full-virus-lockdown-enforced-by-army-817215.html> (accessed 1 Aug 2020).

¹⁰ Andra Timu and Irina Vilcu, "Romania Drafts in Army to Run More Hospitals Amid Virus," Bloomberg News (14 Apr 2020): <https://www.bnnbloomberg.ca/romania-drafts-in-arm-to-run-more-hospitals-amid-virus-1.1421197> (accessed 1 Aug 2020).

¹¹ Photo Source: Presidency.ro, Romania-Insider.com (30 Mar 2020).

¹² "Coronavirus Pandemic: Romanian Military Academy Designs Mechanical Ventilator," Romania-Insider.com (7 May 2020): <https://www.romania-insider.com/ventilator-ferdinand-military-academy-may-2020> (accessed 1 Aug 2020).

- ¹³ “Newsflash,” Radio Romania International (21 Mar 2020): https://www.rri.ro/en_gb/march_21_2020-2614092 (accessed 1 Aug 2020).
- ¹⁴ “COVID-19 Pandemic: Romanian Defense Contractors Design and Produce Thermal Scanner,” Romania-Insider.com (9 Apr 2020): <https://www.romania-insider.com/scanner-pro-optica-ior-covid> (accessed 1 Aug 2020).
- ¹⁵ U.S. Army, “The Army Protection Program,” Army Regulation 525-2 (8 Dec 2014), Headquarters, Department of the Army, Washington, D.C., pp. 6-7.
- ¹⁶ “Army Protection Program,” Stand-To! The Official Focus of the U.S. Army (30 Dec 2014): https://www.army.mil/standto/archive_2014-12-30/ (accessed 1 Aug 2020).
- ¹⁷ Yanzhong Huang, “U.S. Dependence on Pharmaceutical Products from China,” Council on Foreign Relations (14 Aug 2019): <https://www.cfr.org/blog/us-dependence-pharmaceutical-products-china> (accessed 1 Aug 2020).
- ¹⁸ Huang.
- ¹⁹ Sautin.
- ²⁰ Frans-Paul van der Putten, “The Balkans and Black Sea Region and China’s New Silk Road,” Clingendael: Netherlands Institute of International Relations (6 Jul 2017): https://www.clingendael.org/sites/default/files/2017-07/Balkans_Black_Sea_Region_and_China_1.pdf (accessed 1 Aug 2020).
- ²¹ “Yevgen Sautin, “China’s Black Sea Ambitions,” Foreign Policy Research Institute (11 Dec 2018): <https://www.fpri.org/article/2018/12/chinas-black-sea-ambitions/> (accessed 1 Aug 2020).
- ²² “Bank of China Ready to Finance Key Highway Project in Romania,” Romania-Insider.com (19 Dec 2019): <https://www.romania-insider.com/bank-china-finance-highway-dec-2019> (accessed 1 Aug 2020).
- ²³ Jessica Brandt and Torrey Taussig, “The Kremlin’s Disinformation Playbook Goes to Beijing,” Brookings (19 May 2020): <https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/> (accessed 1 Aug 2020).
- ²⁴ “Center of Excellence (COE) Catalog 2020”, NATO (2020): <https://www.act.nato.int/images/stories/structure/coe-catalogue-2020.pdf> (accessed 1 Aug 2020)
- ²⁵ “Digital Economy and Society Index Report 2018,” European Commission (2018): https://ec.europa.eu/information_society/newsroom/image/document/2018-20/1_desi_report_connectivity_DFB52691-EF07-642E-28344441CE0FCBD1_52245.pdf (accessed 1 Aug 2020)
- ²⁶ “Digital Economy and Society Index Report 2018”.

IDENTITATEA NAȚIONALĂ – ÎNTRE NAȚIONALISM ȘI MULTICULTURALISM

Cristian DOBRE*

Abstract

The purpose of this article is to explore, with the methods of psychology, to what extent the concept of “national identity” still holds true nowadays and what its role will be in the future.

To illustrate this, we propose a general overview of the current security environment, followed by a multi-layer analysis of the concept, introducing consecutive layers that give it consistency and define it.

The analysis places “national identity” between two other concepts, “nationalism” and “multiculturalism”, and seeks to identify where it is found today, in the context of the major social and political changes that mark the 21st century.

Last but not least, the article hopes to identify the link between “national identity” and “national security” and to propose some directions for action.

Keywords: national identity, multiculturalism, nationalism, psychology, national security.

Care este contextul în care se supune atenției conceptul de „identitate națională”?

Descrisă din ce în ce mai frecvent de acronimul VUCA (Vulnerability, Uncertainty, Complexity, Ambiguity), concept introdus de U.S. Army War College, la începutul anilor '90, pentru a descrie mediul internațional de securitate post-Război Rece, lumea în care trăim se străduiește, parcă, să-i confirme validitatea, cu fiecare ocazie.

Astfel, separării și reconfigurării unor țări, cum ar fi Uniunea Sovietică, Iugoslavia, Cehoslovacia, Congo, Sudan etc., le-au succedat proclamările unilaterale ale independenței unor regiuni (Abhazia, Osetia, Transnistria etc.) ce aparțineau unor state suverane, cu ajutorul unei puteri externe, urmate de anexarea, prin forță, a unor teritorii ale altor state (de exemplu, Peninsula Crimeea), pentru ca, în trecutul foarte apropiat, mișcările secesioniste din tot mai multe state să devină extrem de active și să

ceară în mod tranșant și unilateral separarea de țara-mamă, cel mai ilustru exemplu fiind cel al provinciei spaniole Catalonia.

La aceste elemente deja enunțate se mai pot adăuga: războiul hibrid de la granițele unor state (de exemplu, Ucraina – Federația Rusă), dezghețarea unor conflicte înghețate (cum ar fi Nagorno-Karabakh), slăbirea până la pierderea totală a autorității statului în țări precum Afganistan, Irak, Libia, Siria, Somalia etc. – în urma unor războaie interne extrem de crude, proclamarea unor entități religioase extremist-teroriste, precum Califatul Statului Islamic, năzuința spre autodeterminare a unor popoare, cum ar fi cele kurd și palestinian, conflictele de graniță – precum cele din regiunea Kașmirului, Etiopiei și Eritreii, Înălțimile Golan etc. și neîncetata luptă pentru revendicarea suveranității asupra unor insule, în special în Marea Chinei de Sud.

*Expert în cadrul Ministerului Apărării Naționale.

Exacerbarea mișcărilor politice centrifuge în cadrul Uniunii Europene (BREXIT, FREXIT, NEXIT, CZEXIT, SWEXIT etc.), asociată cu ascensiunea la putere a unor forțe politice radicale de extremă dreaptă în unele țări europene, apariția unor mișcări publice puternice anti-imigrație, în paralel cu amplificarea până la nivel de criză a acestui fenomen, enclavizarea orașelor occidentale cu populații de emigranți islamici care refuză integrarea în societatea de adopție, eșecul unor politici comunitare de impunere a „cotelor obligatorii de imigranți statelor membre ale UE”, concomitent cu producerea unor atentate teroriste sângeroase (Franța, Germania, Rusia, Turcia, Bulgaria, SUA etc.) – au accentuat percepția incertitudinii până la nivel de individ.

Aceste fenomene psiho-socio-politico-demografice se derulează pe fondul unui mediu de securitate deja marcat de atentatele teroriste împotriva SUA din 11 septembrie 2001, de criza economico-financiară din 2007-2009, de reconfigurarea jocurilor geo-strategice (Rusia-Turcia, Iran-Occident, China-SUA, Turcia-UE, Serbia-Rusia, China-Rusia etc.), de acțiuni populiste (în Balcanii de Vest), de rivalități tradiționale (Rusia-SUA, China-Japonia etc.), de ajustarea sferelor de influență ale marilor puteri și ale unor actori regionali (Rusia, China, Turcia, Iran, Arabia Saudită, SUA), de gestionarea deficitară a crizei emigranților de către liderii europeni (migrația din Siria, Afganistan, Nordul Africii), de acutizarea disparităților economico-financiare dintre statele G7/ G20 și restul lumii, de re poziționarea geo-politică și economică a unor state în arhitectura internațională (China, Rusia, Turcia, Polonia, Coreea de Nord, Vietnam etc.), de degradarea accelerată a mediului înconjurător – în contextul în care unele țări s-au retras unilateral din acordul internațional de protejare a mediului de la Paris, de catastrofe naturale (cutremure, inundații, erupții vulcanice de proporții), de pandemii (SAR, gripa porcină, Zika etc.), de dezastre tehnologice (de exemplu, accidentul de la centrala nucleară de la Fukushima), de exacerbarea acțiunilor xenofobe, naționalist-rasiste (exprimate prin agresiuni la adresa imigranților sau religiei/culturii acestora,

genocid etc.), de intensificarea acțiunilor de criminalitate transfrontalieră și a acțiunilor de subminare a intereselor economice legitime ale unui stat (organizații de traficanti de arme, droguri, carne vie, bunuri de contrabandă, economia neagră etc.), de perturbarea culoarelor energetice strategice ale lumii (de exemplu, oprirea gazului rusesc către Occident), de inconsecvență europeană și concurență acerbă în trasarea noilor rute de transport pentru hidrocarburi și energie electrică, de atacuri cibernetice de amploare la adresa unor instituții guvernamentale, bancare, economice, politice, militare și de presă, de acțiuni subversive, de dezinformare sau informare ostilă destinate subminării și discreditării autorităților legitime ale unui stat, polarizării și radicalizării societății, erodării spiritului civic, coeziunii și solidarității sociale, de acte de piraterie pe mare pe traseul rutelor strategice de transport internațional, de migrația masivă a forței de muncă - cu consecințe dramatice în plan economic și de securitate națională, de amestecul grosolan în treburile interne ale altor state, de acțiuni de proliferare nucleară (de exemplu, Coreea de Nord), de declinul demografic accentuat în Europa - cu consecințe evidente de schimbare a culturii și a stilului de viață tradițional european, urmare a înlocuirii treptate a populației native – fapt ce le potențează efectele și le mărește nivelul de complexitate și impredictibilitate la cote alarmante.

Aceste situații, prezente în realitatea contemporană, sunt amplificate de fenomenul „globalizării”, fenomen ce și-a arătat, deopotrivă, atât fațeta pozitivă, cât și cea negativă. Cea de-a doua, însă, s-a dovedit a fi extrem de dificil de gestionat la nivel planetar, urmare a unor factori precum: precaritatea resurselor Terrei, fractura ideologică ireversibilă dintre sistemele de securitate mondiale (ex. SUA-Rusia), fragmentarea ireconciliabilă religios-dogmatică (sunniți-șiiți, creștini-musulmani, budiști-musulmani, agnostici/atei-credincioși etc.), interesele divergente ale actorilor statali (cele 195 de state suverane) și non-statali (corporații internaționale, state nerecunoscute de ONU, organizații teroriste, ONG-uri, organizații oculte,

religioase, criminale etc.), în demersul lor de a avea acces la resursele planetare, lipsa de capital a țărilor deținătoare de resurse naturale brute pentru a și le exploata cu propriile forțe etc.

În acest context, poziția geostrategică a României, la granița de Est a NATO și UE și la confluența unor sisteme de securitate radical opuse, reprezintă, în egală măsură, un risc, o vulnerabilitate, dar și o oportunitate, în contextul discutării conceptului de „identitate națională”.

Cunoașterea în detaliu a acestor elemente, înțelegerea lor și prognozarea cu precizie a celor ce vor urma, în vederea prevenirii surprinderii strategice, reprezintă misiunea de bază a serviciului de informații militare.

Care este accepțiunea cea mai comună a conceptului de „identitate națională”?

Concept cristalizat, cu precădere, în secolul al XIX-lea, identitatea națională are în limba română un sens relativ asemănător cu cel de „conștiință națională” și de „sentiment național”.

Deși nu există o definiție unanim acceptată a „identității naționale”, cei mai mulți autori agreează ideea că acest concept se referă la sentimentul liber consimțit de apartenență la un stat sau/și națiune. Sintagma de referință poate avea mai multe sensuri: psihologic, tehnic și moral.

Astfel, *sensul psihologic* aduce în prim-plan elementul conștiinței de sine, prin prisma diferenței dintre „noi” și „ei”. *Sensul tehnic* are în vedere aspectele de natură legislativă și se asociază cu naționalitatea, etnia, religia, limba, emiterea documentelor de identitate, îndeplinirea obligațiilor legale față de un stat, dreptul de ședere pe un teritoriu anume, apărarea intereselor personale și colective, legăturile de sânge/rudenie etc. *Sensul moral* se referă, cu precădere, la latura subiectivă a identității naționale și cuprinde un ansamblu de sentimente, emoții, valori, cutume, dogme, ideologii, cultură, religie, simboluri naționale, istorie etc. – care definesc atât individul, cât și grupul de apartenență al acestuia. De regulă, acest ultim sens este intens politizat și i se asociază concepte precum patriotismul, eroismul, loialitatea, trădarea, apărarea intereselor naționale etc.

Rupert Emerson (1960) descria identitatea națională ca fiind acel sentiment ce apare într-o „masă de oameni ce are credința că aparține unei națiuni”, în timp ce sociologul Anthony Smith (1991) o descrie ca pe un rezultat al unui proces profund de socializare ce se poate transmite de la o generație la alta.

Așadar, în opinia noastră, **identitatea națională** este acel concept ce leagă o persoană, prin mecanisme psiho-sociale, politico-administrative și morale, de un grup uman în care se regăsește pe sine prin intermediul apartenenței la un stat și al comuniunii de limbă, tradiții, cultură, teritoriu, istorie, trăsături psiho-morale.

Care sunt straturile ce compun „identitatea națională” și cum se manifestă acestea?

După cum s-a menționat mai sus, identitatea națională este un concept complex, ce presupune existența mai multor „straturi” ce se pot adăuga succesiv, concentrându-i înțelesul.

În anumite situații, însă, straturile de referință o pot goli de conținut sau îi pot adânci misterul și nivelul de complexitate – așa după cum se va vedea din cele ce urmează.

În accepțiunea cea mai generală, analiza identității naționale se relaționează, într-o mare măsură, cu apariția națiunilor și presupune suprapunerea următoarelor planuri:

Planul lingvistic. Treptat, oamenii au început să conștientizeze că datorită faptului că vorbesc aceeași limbă se pot înțelege bine între ei. Limba, însă, a fost afectată și schimbată, în diferite măsuri, de influențele triburilor migratoare, ale marilor cuceriri, de dominația imperială, de descoperirile tehnico-științifice, de apariția tiparului, de dezvoltarea mijloacelor mass-media și a comunicării la distanță, de elemente de natură geo-politică și nu numai. În același timp, limba a contribuit, într-o măsură covârșitoare, la agregarea celor mai multe dintre țările din zilele noastre, inclusiv a României.

Puterea limbii în definirea identității naționale este dată de exemplul populațiilor care, deși trăiesc de generații pe alte teritorii și aparțin de jure unui anumit stat, de facto se percep pe sine

ca aparținând statului a cărui limbă o vorbesc, cum ar fi, de exemplu, comunitatea turcă din Germania.

Limba continuă să joace un rol fundamental în consolidarea identității naționale, însă există și excepții notabile pe plan internațional, date de faptul că anumite populații deși vorbesc limbi diferite au conștiința identității naționale, cum ar fi Elveția, Canada, India, după cum aceeași limbă este vorbită în mai multe țări, dar fiecare dintre populațiile respective au percepții total diferite cu privire la identitatea lor națională (engleza este limbă oficială în peste 60 de țări, iar franceza în peste 30).

Planul politico-administrativ. Acest plan se referă la apartenența formală a subiecților la un anumit stat, prin intermediul cetățeniei, a documentelor oficiale de identificare, a puterii de aplicare a legii și autorității statului de referință, a pârgurilor economico-financiare, a accesului la resurse, a modului de asigurare a securității individuale și colective de către puterea statală, a modului de exercitare a drepturilor și obligațiilor și de respectare de către stat a drepturilor fundamentale ale omului, de participarea indivizilor la viața politică și socială a entității de referință.

La acest plan mai contribuie conceptele de „independență”, „suveranitate”, „integritate teritorială”, care potențează conceptul de identitate națională.

Acest plan se impune, de cele mai multe ori, natural în conștiința subiectului, doar prin faptul că s-a născut într-un anumit stat sau pentru că părinții ori rudele sale sunt cetățeni ai statului respectiv.

Pentru cei mai mulți români, cetățenia română reprezintă un element suficient de puternic pentru a le întări sentimentul identității naționale.

Însă, și în acest plan sunt excepții: astfel, unii oameni nu au conștiința identității naționale, urmare a faptului că societatea la care ei se raportează este una tribală, ce le oferă un sentiment de apartenență mult mai puternic decât cel solicitat de stat. Astfel de cazuri sunt des întâlnite în Afganistan, Pakistan și nu numai.

Tot în rândul excepțiilor se regăsesc situațiile când o persoană aparține mai multor state (are cetățenie multiplă), ori nu aparține niciunui stat (apatrid), ori a renunțat la o cetățenie în favoarea alteia sau nu recunoaște puterea legitimă dintr-o anumită țară (este dizident, insurgent etc.).

Percepția identității naționale poate fi diminuată/perturbată și în situația în care o persoană provine dintr-o familie ai cărei părinți aparțin unor state diferite, ea însăși putând să locuiască într-o terță țară ori în cazul în care statul de apartenență s-a destrămat din diverse motive, iar persoana în cauză a fost obligată să dobândească arbitrar o anumită cetățenie (de exemplu, cetățenia iugoslavă, urmată de cetățenia bosniacă).

La aceste excepții mai pot fi adăugate cele ale persoanelor care trăiesc în anumite teritorii nerecunoscute de către statul-mamă ori/și de către comunitatea internațională, ele având în această situație o cetățenie autoatribuită vremelnic și unilateral, cum ar fi, de exemplu, cetățenii care locuiesc în Taiwan, cei din Transnistria etc. În asemenea situații, locuitorii de referință pot avea percepția identității naționale raportată la regiunea în care trăiesc, dar aceasta este una deformată de contextul geopolitic al momentului.

Planul istoric. Acest plan reunește memoria colectivă a generațiilor anterioare, care au contribuit la construirea națiunii de referință. Bătăliile militare și politice, greutățile și succesele economice, politice, militare, sociale, rezistența în fața cuceritorilor și lupta de eliberare, propriile cuceriri, sunt elemente ce construiesc planul istoric. Acesta se fundamentează pe descoperiri arheologice și alte izvoare istorice și este reflectat, cel mai frecvent, în cultul eroilor neamului, care întreține sentimentele de mândrie națională și patriotism.

În cazul României, istoria sa multimilenară, asociată cu lupta pentru unitatea națională, pentru independență și eliberarea de sub diferiți stăpâni ai momentului, împreună cu o galerie considerabilă de eroi, însuflețește puternic percepția identității naționale.

Este remarcabil faptul că planul istoric a reușit să mențină sentimentul identității naționale

peste generații, la populații ce au trăit pentru decenii sub autoritatea unui stat terț (de exemplu, Transilvania, fostele republici sovietice, statele componente ale fostei Iugoslavii etc.).

Planul cultural. Constituit din totalitatea valorilor materiale, spirituale și intelectuale create de o comunitate umană, acest plan reprezintă un puternic catalizator al identității naționale. El poate include viziuni asupra lumii, credințe, basme, mituri, povești, ideologii – exprimate prin *forme tangibile*, de natură materială, precum înscrisuri, picturi, sculpturi, mobilier, instrumente muzicale, mâncăruri specifice asociate cu rețete culinare unice, creații tehnico-științifice, tipuri de locuințe, invenții, ținute, simboluri (steag, stemă, blazon, uniformă militară, port popular etc.) etc. sau *intangibile*, de natură spirituală sau intelectuală – exprimate prin valori, filozofii, teorii, ideologii, cântece, poezii, teatru și cinematograf, vorbire, dansuri, obiceiuri, tabuuri, cutume, moravuri, superstiții, divertisment, comportamente manifeste etc.

Într-o anumită măsură, acestui plan i se subordonează și învățământul, văzut ca o formă a culturii de masă. Acesta poate transmite, în mod organizat și de cele mai multe ori formalizat, acele elemente pe care factorii de putere ai unui stat îi consideră necesari pentru apărarea intereselor țării sau ale vreunui lider (în cazul dictaturilor).

Planul cultural reprezintă un alt element de rezistență, în pofida oricăror impuneri forțate, el supraviețuind miraculos în cele mai dificile condiții. Astfel, sclavii africani din America și-au păstrat identitatea culturală peste secole și generații, așa cum și populațiile ce au făcut parte din tot felul de imperii au supraviețuit ca entități distincte atunci când imperiile s-au destrămat. Acest plan reprezintă o resursă fundamentală a identității naționale.

În anumite situații, însă, pentru perioade limitate de timp, planul cultural poate fi influențat puternic prin mijloace propagandistice adecvate, dovadă fiind exemplele istorice oferite de al Treilea Reich, de „omul nou multilateral dezvoltat” al regimului comunist din România, de proletarul veșnic supărat pe capitaliști, de filozofia de război antiamericană, anti-japoneză și antisud-coreeană a Coreii de Nord etc.

Acest plan poate fi politizat foarte ușor și poate produce efecte educative puternice la tânăra generație, ce se reflectă în percepția identității naționale.

În anumite situații, modernizarea unei țări impune schimbări culturale dramatice, ce pot avea consecințe sociale și politice de lungă durată, cum ar fi, de exemplu, modernizarea și laicizarea Turciei, pe timpul președintelui Atatürk.

Mișcările libere ale populațiilor la nivel planetar, dezvoltarea mijloacelor de telecomunicație, a mass-mediei, a Internetului și a rețelelor de socializare, precum și promovarea, cu consecvență, în spațiul public a unor valori și obiceiuri, au omogenizat, într-o oarecare măsură, în special la tânăra generație, modalitatea de percepție a realității contemporane și sistemul de gândire, astfel că au fost importate/exportate sărbători, valori, comportamente, stiluri de viață.

Pe de altă parte, menținerea decalajelor economico-financiare majore dintre Occident și Orient, dintre Nord și Sud, promovarea unor repere culturale relativ distincte (colectivism versus egocentrism) și a unei filozofii de viață diferite între punctele cardinale ale planetei, concomitent cu provocările actuale ale mediului de securitate și interesele deseori contradictorii ale marilor actori statali ai momentului, au creat confuzii majore, fapt ce a împins conceptul de „identitate națională” spre zona naționalistă, ca o reacție de autoprotecție și ca un refugiu în conservatorismul clasic.

Planul religios. Înrudit cu cel cultural, acest plan se construiește în timp și se impune cu mare forță prin intermediul instituțiilor ecleziastice și comunității în care trăiește fiecare persoană, începând cu familia. Religia păstrează, de cele mai multe ori, în forma cutumelor și obiceiurilor, reguli stricte de comportament și de exprimare a gândurilor, inclusiv a concepției despre lume și viață și de apartenență la o anume comunitate. Alimentat sistematic din copilărie, sentimentul religios se dezvoltă natural odată cu maturizarea persoanei, dominându-i toate comandamentele.

Unele religii se impun autoritar și incisiv în societate, funcționând paralel cu statul laic sau, chiar, subordonându-l total (Iran, Arabia Saudită,

Emiratele Arabe Unite etc.), în timp ce altele se manifestă mai discret, lăsând liberului arbitru al fiecărei persoane să decidă în ce măsură se va implica în activități religioase sau nu.

Credințele religioase pot genera cele mai intense emoții și pot polariza cu ușurință masele într-o anumită direcție, chiar radicalizându-le, în numele Divinității – oricare ar fi aceasta, pentru atingerea unui anumit interes de moment. În acest fel, extremismul religios devine lesne o formă perfectă de manipulare și de subordonare necondiționată a voinței enoriașilor pentru a fi utilizați în scopuri (auto)distructive, discreționare, teroriste (Al-Qaeda, Statul Islamic, Boko Haram, Al-Shabab, secta Templul Popoarelor, secta Adventiștii Davidieni etc.) sau pentru impunerea intereselor politico-militare în anumite teritorii (budiști versus musulmani în India-Pakistan, catolici versus ortodocși versus musulmani în fosta Iugoslavie, șiiți versus sunniți în Irak, catolici versus protestanți în Irlanda etc.).

Planul etnic. Acest nivel reunește colectivități ale căror membri au, în realitate sau presupun că au, origini și amintiri comune și împărtășesc același trecut istoric și aceeași cultură/religie. Aceste comunități pot forma popoare, dacă au și un teritoriu de viațuire comun. Etniile pot funcționa, așadar, în cadrul poporului/națiunii sau dispartate pe alte teritorii, în calitate de minorități sau diaspore.

Uneori, în cadrul grupurilor etnice se pot regăsi și aceleași rase umane, dar nu obligatoriu, având în vedere că cercetările antropologice recente au demonstrat că noțiunea de „strămoș comun” al grupurilor etnice este mai mult o structură de natură socio-culturală decât una de natură genetică.

În anumite situații, planul etnic poate deveni foarte cuprinzător, reunind subiecți cu origini rasiale, limbi materne, convingeri politice și clase sociale diferite – cum ar fi, de exemplu, comunitatea evreilor, care se autodefineste ca un grup distinct, fără, însă, să facă notă discordantă față de societatea în care trăiește.

În alte situații, grupul etnic, deși deține un teritoriu bine delimitat și formează un popor, nu este recunoscut de statele pe teritoriul

cărora funcționează, ca în cazul kurzilor, sau este determinat să emigreze din statul unde funcționează, ca în cazul minorității musulmane rohingya din Myanmar, care s-a refugiat în Bangladesh, pe motive de natură religioasă.

Uneori, grupurile etnice care viețuiesc pe teritoriile altor state se constituie în minorități puternice, extrem de active, care fie militează pentru a beneficia de aceleași drepturi cu ale majorității, fie doresc să se autoizoleze și determină veritabile mișcări de autodeterminare, ele însele devenind intolerante cu alte minorități etnice ce viețuiesc în mijlocul lor. Așadar, și planul etnic poate alimenta consistent conceptul de „identitate națională”, fără însă a-l explica în totalitate.

Planul psiho-moral. Acest plan reprezintă, în mare parte, o rezultată a celorlalte „straturi”, urmare a faptului că el reușește să mobilizeze și să activeze componentele psihologice emoțional-atitudinale și comportamental-acționale, de la nivel macro-grupal și până la nivel individual.

Planul psiho-moral funcționează ca un adevărat furnal energetic în care se topesc celelalte componente și care toarnă în forme emoții, comportamente și valori morale, profund subordonate conceptului de „identitate națională”, încercând să le promoveze pe cele elogiante, cum ar fi patriotismul, eroismul, datoria față de țară, loialitatea, determinarea, hotărârea, curajul, onoarea, integritatea, spiritul de sacrificiu, încrederea, perseverența, respectul, credința, entuziasmul, ingeniozitatea, spiritul justițiar, ordinea, ospitalitatea, punctualitatea etc., și să le elimine pe cele repugante: trădarea, lașitatea, inconsecvența, indiferența, teama, frica, zgârcenia, lenea, coruptibilitatea, infidelitatea, egoismul, lăcomia, iresponsabilitatea, ipocrizia, grosolănia etc.

Acest plan poate fi și el ușor manipulat ideologic/dogmatic atât la nivel statal, cât și la nivel sub-statal, pentru atingerea unor interese bine ținute.

Exemplele de loialitate supremă oferite de piloții japonezi kamikaze împăratului lor în al Doilea Război Mondial, asemeni milioanelor de soldați din toate taberele militare, care au

pus interesul național și misiunea militară mai presus de propria lor viață, sunt dovezi concrete ale conținutului faptic ce umple conceptul de „identitate națională”.

Acest concept mai poate fi jucat însă și politic, rasial, național, etnic, economic, militar, religios, cultural, media etc. – în funcție de anumite interese. Un exemplu ilustrativ ar fi „patriotismul”, care a fost invocat de-a lungul istoriei umanității de foarte multe ori, pentru a justifica, deopotrivă, acțiuni mărețe, respectiv acte oribile de barbarie (distrugerea orașelor, uciderea populației civile, discriminări de proporții epice, deportări etc.). Excesul de patriotism poate conduce uneori la extremism, naționalism și chiar terorism, în anumite condiții.

Mai nou, unele *think-thank*-uri doresc să-i atribuie patriotismului o vocație globală – aceea potrivit căreia „a fi patriot” înseamnă să respecti patria tuturor, adică Pământul însuși, menținându-l curat, ecologic și protejând, în egală măsură, toate viețuitoarele ce trăiesc pe această planetă.

Care este perspectiva psiho-socială a „identității naționale” raportată la conceptele de „naționalism” și, respectiv, „multiculturalism”?

Prin excelență o doctrină politică, cristalizată începând cu secolul al XVIII-lea, *naționalismul* a adus în prim-plan conștiința națională și a constituit motorul formării națiunilor și statelor naționale. În anumite circumstanțe, exacerbarea sa i-a deformat sensul nobil inițial și l-a radicalizat în ideea întreținerii urii de rasă și naționalitate, formării exclusivismului național în raport cu alte națiuni, transformându-l într-un concept monstruos, urmare a formelor sale de șovinism, rasism, hegemonism, xenofobie, egocentrism național, care au condus adesea la atrocități, conflicte interne și interstatale sângeroase.

Multiculturalismul, ca și doctrină politică apărută în anii '30, presupune coexistența pașnică, armonioasă, înțelegerea mutuală și complementară a mai multor culturi, etnii, grupuri religioase diferite în același spațiu geografic. Spre deosebire de alte curente politice ce militează pentru integrare socială, segregare rasială, asimilare

culturală, multiculturalismul militează pentru păstrarea caracterului distinctiv al fiecărei culturi, fiind deseori asemuit conceptului de „mozaic cultural”. În anumite circumstanțe, exacerbarea multiculturalismului i-a deformat sensul nobil inițial și l-a radicalizat în ideea enclavizării/izolării unor culturi ce conviețuiesc împreună cu alte culturi, creșterii nivelului concurențial inter-cultural în întrecerea pentru resurse, locuri de muncă, demnități publice, accesul la putere, demonstrarea superiorității etc., spre negarea autorității legitime a unui stat suveran în numele multiculturalismului, spre dizolvarea completă a autorității statului în favoarea federalizării unei regiuni sau a unui număr de țări ce aparțin deja unei anume organizații regionale.

Așadar, se observă că ambele concepte mai sus descrise pot fi deformate și radicalizate în forme sociale anomice și extremiste. Astfel, dacă ar fi să plasăm pe o scală naționalismul, identitatea națională și multiculturalismul, cu siguranță la ambele capete ale scalei am așeza „extremismul”, iar la mijloc „identitatea națională”, probabil gravitând între naționalism și multiculturalism, în funcție de capacitatea de autocontrol și toleranță a fiecărei societăți.

Din punct de vedere psihologic, mecanismele percepției, emoțiile, atitudinile, opinia, concepția despre lume și viață, capacitatea cognitivă de a analiza realitatea vor juca roluri majore în oscilațiile conceptului de „identitate națională” pe scala de referință.

Unele dintre organizațiile internaționale, cum ar fi ONU, NATO, OSCE etc., militează pentru păstrarea identității naționale a fiecărui stat, în contextul aderării acestuia la un set de valori și principii universal ori regional acceptate. Pe de altă parte, alte organizații sau grupuri de interese militează pentru radicalizarea conceptului de „identitate națională” invocând, în mod pervers, anumite elemente, tendențios selecționate, din nivelele sale constitutive, ca argumente. În acest context, se pot descrie pentru exemplificare și mișcările centrifuge anti-Uniunea Europeană, care invocă deopotrivă argumente raționale și emoționale pentru a explica dizolvarea organizației sau extragerea țării lor din aceasta.

Complexitatea, impredictibilitatea, incertitudinea și vulnerabilitatea mediului actual de securitate pot influența și deruta ușor mase largi de oameni, care pot susține, chiar în necunoștință de cauză, obiective sociale, economice și politice nerealiste, deplasate cu ușurință spre zonele extremismului, indiferent cum s-ar numi el. Manipularea, propaganda, ingineria opiniilor, managementul comportamentelor și psihologia maselor pot reprezenta tot atâtea forme ale agresiunii psihologice destinate să implementeze interesele unor minorități în defavoarea popoarelor din statele suverane sau al organizațiilor mai sus menționate.

O analiză pragmatică și lucidă a realității contemporane, din care „stratul” psiho-social al PSYINT-ului nu ar trebui să lipsească, ar putea prognoza din timp astfel de tendințe periculoase și formula cursuri de acțiune echilibrate, din care liderii de nivel înalt să aleagă soluția cea mai bună.

Este vreo legătură între „identitatea națională” și „securitatea națională”?

Concept de o cuprindere exhaustivă foarte generoasă, „securitatea națională” include subdomenii diverse, printre care se numără securitatea economică, alimentară, a sănătății publice, a energiei, internă, militară, cibernetică, a resurselor minerale și de hidrocarburi, a surselor de apă, a mediului, socială, demografică, informațională ... și lista ar putea continua.

În acest concept, fără îndoială și-ar găsi locul și „identitatea națională”, în calitate de liant al domeniilor mai sus enunțate și menținerii unității, integrității și inviolabilității statului suveran, ca parte la organizațiile la care acesta s-a alăturat liber consimțit.

Și totuși, odată cu aderarea României la Uniunea Europeană și la Alianța Nord-Atlantică, o parte a suveranității naționale a fost cedată organizațiilor de referință, în interesul comun al fiecărui stat membru și al alianțelor de referință, ca și întreg. În aceste condiții, identitatea națională continuă să se manifeste în cadrul conceptelor de „unitate în diversitate” (motto al UE, din anul 2000) și „animus in consulendo

liber” (ultimul motto al Alianței), formularea unor interese naționale pertinente și urmărirea lor cu transparență și consecvență în parcursul european și euro-atlantic al țării va consolida identitatea națională a fiecărui cetățean.

Totodată, cunoașterea, la nivel general, a evoluției conceptului, indiferent de țară, poate permite o mai bună înțelegere a evoluției mecanismelor de securitate la nivel planetar.

Ce este de făcut cu ... „identitatea națională”?

Se apreciază că identitatea națională va continua să rămână o puternică sursă psiho-energetică pentru generațiile viitoare, în pofida proceselor de globalizare/mondializare tot mai intense, a încercărilor de unificare a unor spații geografice și în contextul unor eșecuri lamentabile de natură economico-financiară, politico-diplomatică și a unor situații de criză generate de cauze diverse (războaie interne, catastrofe naturale ori tehnologice, colaps economico-financiar, conflicte locale etc.).

Se estimează că statele vor continua să-și mențină rolul de catalizator al resurselor umane și materiale pe care le înglobează, iar cedarea unor prerogative ale suveranității în favoarea unor organizații regionale ar trebui gestionată cu mare prudență, pentru a nu leza identitatea națională.

Alunecarea conceptului, pe axa mai sus descrisă, spre oricare dintre capetele sale consacrate extremismului va constitui un veritabil semnal de alarmă pentru acțiuni imediate de reconciliere, de pacificare și de detensionare a situației, indiferent dacă ea va apărea la nivel intra-statal ori interstatal.

Totodată, identitatea națională poate fi degradată sau chiar pierdută în contextul în care se importă nediscriminativ elementele sale constitutive, cu accent pe cele culturale, din alte părți ale lumii, urmare a transformării cetățenilor în consumatori necritici și obedienți ai unor produse finite, aparent mai ușor de „digerat cultural”.

Identitatea culturală va rămâne vulnerabilă la agresiunea psihologică, dar, în condițiile unei educații solide a cetățenilor, acest risc poate fi diminuat sau chiar prevenit.

Punerea la dispoziția decidenților politico-militari și militari a unor produse de intelligence veridice, exacte, necesare, clare, oportune, fiabile, pragmatice și dedicate, care să evidențieze și evoluțiile internaționale în planul psiho-social și, cu precădere, al identității naționale va asigura o bună înțelegere a imperativelor mediului de securitate actual și va asigura garanția luării unor hotărâri adaptate contextului de referință.

Printr-un management inteligent de tip VUCA (Vision, Understanding, Clarity și Agility) al provocărilor la adresa mediului de securitate actual, descrise la începutul acestui articol, se poate obține o adaptare mai eficientă a conceptului de „identitate națională” la realitatea contemporană.

Așadar, gestionarea identității naționale va constitui o competență și o datorie a oricărui stat responsabil, care se respectă și are interese bine definite.

Bibliografie:

1. ANTONSICH, Marco&Michael Skey (2017), *Everyday Nationhood: Theorising Culture, Identity and Belonging after Banal Nationalism*, Palgrave Macmillan UK.
2. BARKER, Fiona (2015), *Nationalism, Identity and the Governance of Diversity: Old Politics, New Arrivals*, Palgrave Macmillan UK.
3. BERGHOLZ, Max (2016), *Violence as a Generative Force: Identity, Nationalism, and Memory in a Balkan Community*, Cornell University Press.
4. BECHHOFFER, Frank; McCrone, David (eds.) (2016), *National Identity, Nationalism and Constitutional Change*, Palgrave Macmillan UK.
5. BLUM, Douglas (2007), *National Identity and Globalization: Youth, State, and Society in Post-Soviet Eurasia*, Cambridge University Press.
6. DOBRE, Cristian (2013), *Psihologie diplomatică*, Editura Universității Naționale de Apărare „Carol I”, București.
7. DOBRE, Cristian (2015), *Dimensiunea psiho-socială a crizei emigranților*, în *Infosfera*, anul VII, nr. 4.
8. EDENSOR, Tim (2002), *National Identity, Popular Culture and Everyday Life*, Berg, Oxford.
9. FAWN, Rick (2003), *Ideology and National Identity in Post-communist Foreign Policy*, Routledge.
10. JONES, Jack (2005), *An Introduction to Factor Analysis and Information Risk (FAIR)*. Risk Management Insight.
11. JOSEPH, John E. (2004), *Language and National Identity: National, Ethnic, Religious*. New York and Hampshire: Palgrave Macmillan.
12. LEE, Yoonmi (2012), *Modern Education, Textbooks, and the Image of a Nation*, London: Routledge.
13. LUCARELLI, Sonia; Manners, Ian (2006) (eds.), *Values and Principles in the European Union Foreign Policy*. Abingdon, Oxon: Routledge.
14. EMERSON, Rupert (1960), *From Empire to Nation*. Boston, MA: Beacon Press.
15. SMITH, Anthony (1991), *National Identity*. University of Nevada Press.
16. ȘERBU, Miliana și Gheorghe, Constantin (2006). *Globalizare și identitate națională*, volum simpozion, Editura MAI, București.
17. WODAK, Ruth; de Cillia, Rudolf; Reisigl, Martin; Liebhart, Karin (2009). *The Discursive Construction of National Identity*, Second edition, Edinburgh: Edinburgh University Press.
18. <http://assets.pewresearch.org/wp-content/uploads/sites/2/2017/04/14094140/Pew-Research-Center-National-Identity-Report-FINAL-February-1-2017.pdf>.

LIMITELE ARANJAMENTELOR POST-CONFLICT. FEUDALIZAREA SECTARĂ ȘI IMPLOZIA SISTEMULUI POLITIC LIBANEZ

*Dr. Iulian CHIFU**

Abstract

Post-conflict arrangements are always welcomed since they provide solutions to very complicated problems by solving the divisions of power inside non-cohesive societies, harmed by ethnical, national and religious, even sectarian divisions. But those creative solutions as those involved in constructive ambiguities have side effects that produce in time new crises, without a possibility to be solved in the existing framework. Lebanon case could give us lessons learnt on how such arrangements that seem panacea are fighting back and weakening a society and a state. And a crisis of the kind Lebanon faces nowadays is exposing those shortcomings. Those experiences should require a more thorough analysis of the effects in time of the administrative, diplomatic and negotiations agreements, due to solve crisis.

Keywords: *post-conflict reconstruction, weak state, failed state, sectarian monarchies, oligarchic sectarianism, longterm effects.*

Sistemul sectar libanez și împărțirea puterii după Războiul civil

Războiul civil din Liban (1975-1990) a fost unul dintre cele mai cunoscute „războaie lungi” care au ajuns la un final, la un acord. Împărțirea funcțiilor pe baze religioase și sectare a stabilit că Președintele statului va fi un creștin maronit, președintele Parlamentului un šiit, iar premierul va aparține comunității sunnite¹. Tipul acesta de aranjamente post-conflict, care soluționează problema împărțirii puterii, s-a regăsit ulterior în multe alte spații, atât în Europa – Bosnia și Herțegovina, cât și în Orientul Mijlociu – Irak. În plus, există o mare posibilitate ca acest tip de aranjament să se repete în Siria; de aceea, lecțiile învățate rezultate recent din criza exploziei catastrofale din Beirut și ceea ce ne spune aceasta despre sistemul libanez de putere trebuie învățate, pentru că ele evidențiază limitele acestor aranjamente de soluționare a unor conflicte prin împărțirea puterii pe baze sectare și religioase și efectele acestui tip de soluție în timp.

Explozia devastatoare din 4 august 2020² de la depozitul de azotat de amoniu din Beirut, unde era depozitată o cantitate aflată acolo de mai bine de șase ani, despre care știau și fuseseră informate toate autoritățile³, subliniază capacitatea administrativă redusă și lipsa de interes a actualei clase politice libaneze, a actualelor elite, în legătură cu siguranța și viața cetățenilor. De la neglijență la corupție, s-au spus foarte multe și au fost recunoscute chiar la nivel oficial⁴, însă mai puține lucruri s-au spus despre sistemul care a dus aici, situat între sectarianism oligarhic și adevărate monarhii, caste sectare care acaparează funcții și poziții fixe în societatea libaneză.

Dacă aranjamentul de împărțire a funcțiilor în Liban datează de la încheierea războiului civil, sistemul sectar și formula de succesiune pe linie familială în conducerea acestor structuri sectare, partide religioase și alte forme de control al comunităților sunt mult mai vechi și datează din perioada colonizării franceze (1920-1943),

**Iulian CHIFU este conf. univ. dr. la SNSPA și UNAp, specializat în Analiză de conflict și Decizie în criză. Este președintele Centrului de Prevenire a Conflictelor și Early Warning. Între 2011-2014 a fost consilier prezidențial pentru Afaceri Strategice, Securitate și Politică Externă.*

după ce Franța a obținut de la Liga Națiunilor mandatul administrării Libanului și Siriei⁵, odată cu prăbușirea Imperiului Otoman, la finele Primului Război Mondial. De atunci, Franța a privilegiat creștinii, cu precădere maroniții⁶, care dominau societatea libaneză și erau prezenți în conducerea tuturor grupărilor creștine. Defavorizați au fost musulmanii, de unde marea explozie a războiului civil, și pe fondul modificărilor demografice⁷.

Firește că istoria e mai lungă și mai complicată: Franța Regimului de la Vichy s-a confruntat și în Liban cu Franța Liberă și Rezistența a câștigat, odată cu independența Libanului în 1943⁸. Iar din 1946, aranjamentul de împărțire a Parlamentului pe cote de creștini și musulmani, ca și a funcțiilor în stat, a fost instalat. De atunci durează marile familii conducătoare în Liban, ale căror strănepoți preiau astăzi de la părinții lor conducerea statului care se dovedește slab și inefficient, gata să eșueze, cu o clasă politică în plină implozie⁹. Motivul principal este această împărțire de funcții și poziții și moștenirea lor din tată-n fiu, prin pervertirea democrației și o formă de feudalizare sectară a statului.

Concret, alegerile nu schimbă fundamental controlul și raporturile de putere, care rămân în aceleași mâini. Se schimbă fețe, personaje, oameni de prim-plan, nicidecum esența feudalizării statului. Și cât timp aceste puteri nu se alocă democratic, fără a ține cont de aranjamente post-conflict, rezultatul este un sistem inefficient, cu clientele sectare și accesul în funcții care nu poate avea loc decât cu aprobarea familiilor deținătoare a controlului asupra propriilor comunități.

Liniile de falie sunt cel puțin la fel de complicate în societatea libaneză: mai întâi cele etnice și religioase, cu profunde controverse și conflicte între ele. Maroniții s-au confruntat cu druzii, încă din secolul 19, și împart zonele muntoase și de nord¹⁰. Maroniții, la rândul lor, au fost implicați în războaie și confruntări interne, pe liniile unificării cu Siria, menținerii legăturii cu Franța și independențe ireale a statului libanez. Apoi, sunniții și šiitiții și-au alimentat propriile reglări de conturi cu zona šiită, disputându-și apartenențe, nu rareori și loialități alternative, față de Iran și Siria, față de pan-arabism sau curente islamiste¹¹. Apariția statului Israel, valorile de

refugiați palestinieni și creșterea numărului de sunniți în Liban au creat, de asemenea, tulburări puternice în timp. Ca și prezența šiitiilor la granița de sud a Libanului și în Valea Bekaa. Implicarea Israelului în afacerile libaneze a devenit, astfel, obligatorie, așa cum au fost implicate marile monarhii din Golf, lumea arabă și susținătorii problemei palestiniene. Liniile de falie s-au complicat în timpul Războiului Rece și cu orientările spre cei doi poli, cu naționalismul arab și mișcările de stânga apropiate cauzei palestiniene și chiar unor partide comuniste în Liban, în timp ce dreapta creștină a fost mai aproape de Occident.

Suma acestor falii a rupt Libanul, iar coeziunea a venit greu și târziu. Nocivitatea sistemelor feudelor religioase și sectare a fost amplificată de către războiul civil, care s-a încheiat cu desființarea milițiilor, dar și cu amnistii care au menținut vechile familii și aranjamente sectare în formatul noilor partide religioase¹². Excepția a constituit-o Hezbollahul pro-iranian, care a rămas un stat în stat, cu propriile reguli, forțe armate, operațiuni militare și de *intelligence*, ba chiar propriile comunicații militare¹³.

Aceste excepții și rolul politic al acestei grupări - considerată mișcare teroristă în multe state occidentale - au complicat și mai mult relaționarea internațională cu Libanul. În plus, implicarea recentă, din ultima decadă, în conflictul din Siria a organizației Hezbollah și prezența a peste un milion de refugiați sirieni au alterat și mai mult și au accentuat problemele libaneze. Acesta este contextul nefast al prăbușirii, eșecului și falimentului sistemului politic și al statului Liban, consemnat cu ocazia exploziei din 4 august a.c.

Catastrofa deflagrației din Beirut și expunerea feudalizării sectare a societății libaneze¹⁴

Explozia devastatoare din capitala Libanului, Beirut, a venit în perioada comemorării și a doliului pentru victimele celor două atacuri nucleare care au încheiat cel de-al Doilea Război Mondial, la Hiroshima și Nagasaki. Comparația impactului a fost realistă: 500 tone TNT este estimarea valorii exploziei¹⁵. Numită ulterior „Cernobîlul Libanului”¹⁶, explozia a expus, de fapt, falimentul sistemului politic libanez, iar

crizele suprapuse și responsabilitatea pentru o asemenea catastrofă industrială duc inevitabil la implozia acestui sistem.

De altfel, sistemul politic libanez a fost deja puternic zdruncinat anul trecut de manifestații de stradă masive, care reclamau plecarea întregii clase politice. Și în prezent alegerile anticipate nu par a fi o soluție decât interimară la sistemul politic sectar corupt și fără capacitate administrativă din Liban, contestat în stradă din nou de mii de protestatari¹⁷.

Autoritățile libaneze au oscilat, inițial, între a aduce în față vinovați locali și a blama intervenții externe. Președintele Michel Aoun - cel mai atacat oficial în protestele publice, ale cărui fotografii au fost rupte și arse în asaltul protestatarilor asupra ministerelor și instituțiilor de stat - a produs două ipoteze: neglijența internă și atac extern. Acesta a solicitat Franței, fosta metropolă colonială a Libanului, imagini din satelit pentru a vedea dacă au existat avioane de război sau rachete în aer în zona exploziei la ora deflagrației. În cazul ultimei ipoteze, ea are la bază dorința de a exporta responsabilitatea, invocându-se o afirmație frugală și nefericită a Președintelui Donald Trump, care a anunțat că știe de la niște generali nenumiți că ar fi vorba despre un atac¹⁸. Și Pentagonul, pe diferite voci, și autoritățile libaneze, în prima parte, și organizația Hezbollah, și Israelul au negat orice implicare.

La originea exploziei a stat, potrivit premierului libanez Hassan Diab, o cantitate de 2750 tone de nitrat de amoniu depozitat lângă port, în centrul orașului, un material foarte instabil la temperaturi mari și în prezența benzinei și compușilor chimici. El fusese confiscat pentru neplata taxelor de la un vas rusesc în 2013, încărcătura fiind destinată mineritului în Mozambic. Experții susțin că incendiul la un depozit de artificii alăturat nu ar fi putut declanșa deflagrația, iar fumul degajat și culoarea oranj a acesteia ar reclama prezența unui material exploziv militar. Hezbollahul a infirmat că ar fi avut un depozit de arme în zonă¹⁹. Ciudat este însă că, în ciuda apelurilor interne și internaționale, Michel Aoun, președintele libanez, a respins varianta unei investigații internaționale²⁰, independente, sub egida ONU, rămânând la cercetările locale.

Hassan Koraytem, directorul general al portului Beirut, și Badri Daher, directorul general al Administrației libaneze a Vămile, au fost arestați, ambii fiind cei care au avertizat de mai bine de zece ori, în ultimii șase ani, asupra riscului prezenței încărcăturii explozive în port, în depozitul aflat în proximitatea zonelor turistice, comerciale și centrale ale orașului. Președintele Michel Aoun a recunoscut că a primit acum câteva săptămâni informația și susține că a ordonat imediat oficialilor militari și din zona de securitate să rezolve problema²¹.

Autoritățile libaneze au pus în arest la domiciliu toți oficialii responsabili de depozitarea și paza azotatului de amoniu din port. Dar responsabilitățile sunt mult mai mari și reclamă analiza acestui ciclu al disfuncționalităților și al furturilor, corupției endemice și impunității principalilor lideri ai milițiilor și grupărilor religioase și sectare care alcătuiesc sistemul de partide din Liban. Iar neglijența e cea mai puțin credibilă dintre variante, în orice caz neacceptată de populația care a trecut vineri, 7 august, la proteste masive împotriva întregii clase politice, cerând ca toți să se retragă²². De altfel, un număr mare de parlamentari, ambasadori și politicieni au demisionat din funcții, cerând crearea unei noi clase politice la Beirut. Și Guvernul Diab și-a prezentat demisia, la patru zile distanță²³.

Implozia clasei politice de la Beirut²⁴

Explozia catastrofală din Beirut a venit într-un moment în care Libanul era deja subiectul a numeroase crize suprapuse, care aduseseră țara pe buza prăpastiei. Mai întâi, sistemul sectar și aranjamentele politice pe baze religioase au blocat opțiunile și alternativele și au exasperat populația. Criza refugiaților sirieni a afectat Libanul, unde peste 30% din populație e constituită din refugiați în urma războiului civil ce durează de zece ani într-o țară care domina, controla și se implica constant în afacerile politice de la Beirut.

Criza refugiaților și proasta gestiune a treburilor publice au dus la o criză economică de amploare în Liban, unde, în octombrie 2019, protestele masive de stradă s-au soldat cu eliminarea lui Saad al-Hariri de la conducerea guvernului și au reclamat chiar incapacitatea guvernului de a gestiona afacerile publice.

Lira libaneză a pierdut 80% din valoare în ultimul an²⁵. Peste aceasta a venit criza pandemiei globale de coronavirus, care a făcut ca victimele Covid-19 să aglomereze spitalele, care au fost luate cu asalt de victimele deflagrației, patru dintre centrele medicale fiind distruse și inutilizabile după explozie.

Suma crizelor suprapuse din Liban și viața de zi cu zi subliniază probleme structurale majore ale *leadership*-ului politic. De altfel, chiar premierul Hassan Diab, când a încercat în timpul protestelor să scape de responsabilitate, cerând alegeri anticipate, a recunoscut „criza politică structurală a țării” și „nevoia de o nouă elită politică și de un nou parlament”²⁶. Pentru că, de fapt, Libanul este rezultatul aranjamentelor și impunității propriilor elite politice.

Războiul civil din Liban s-a încheiat în urmă cu 30 de ani, dar greșelile de la terminarea acestuia se regăsesc și astăzi. Aranjamentele au impus supraviețuirea liderilor milițiilor religioase care au schimbat uniforme de diferite facturi în haine și poziții în partidele religioase, în timp ce împărțirea sectară și religioasă a funcțiilor în stat a împietrit și înghețat sistemul libanez, oferindu-l pe tavă grupurilor sectare și vechilor rivalități.

Suma acestor particularități arată că încremenirea în proiect și lipsa soluțiilor politice trans-sectare și trans-religioase, a unei democrații electorale clasice, au dus la propagarea neglijenței criminale, la lipsa capacității administrative, la incompetență și corupție, la o clasă politică ce se îmbogățește fără nicio preocupare față de populație și cu formule de arivism politic datorat exclusiv loialităților față de partidele religioase și sectare, conduse de vechii comandanți transformați în oligarhi kleptocrați. Sistemul de aranjamente, care a dus la acordul privind încheierea războiului civil din Liban în 1990, s-a dovedit falimentar și neadecvat astăzi pentru că a generat, în timp, perpetuarea feudelor politice arvunit sectar și a grupărilor de loialitate religioasă care blochează opțiunile democratice, împropățarea sistemului și care împinge spre implozie.

Nu întâmplător, manifestațiile de protest trans-sectare din octombrie 2019 au reclamat, prin strigătele a milioane de oameni, „kulyan-yani-kulyan” – toți înseamnă toți²⁷, cu referire la plaga împărțirii instituțiilor între partide sectare

și la plaga corupției, a opresiunii, a aranjamentelor interpartinice fără legătură cu realitățile și voința populației. Câteva figuri politice au dispărut sau s-au retras, au fost înlocuite, dar același sistem a continuat să domine Libanul, de unde corupția opresivă și inadecvarea liderilor, incompetența funcționarilor și inacțiunea instituțiilor. Nu întâmplător, ministrul de externe libanez, Nassif Hitti, a demisionat în ajunul exploziei și a invocat „alunecarea Libanului de astăzi spre un stat eșuat”²⁸.

Abordarea disperată a mulțimii furioase pe care am văzut-o în protestele de la Beirut arată lipsa oricăror forme de opoziție organizată. Mișcările civice sunt puține și rare, legate de partidele religioase, iar puterea formală este împărțită între Puterea și Opoziția clasică, instituționalizată, dată de alegeri, în forme fără transparență față de public. Nemulțumirea publică și formulele de protest seamănă mai degrabă cu implozia sistemului politic din Algeria și apariția mișcării de protest Hirak după eliminarea de la putere a președintelui Abdelaziz Bouteflika. Mișcarea algeriană fără lideri a căutat, și caută în continuare, decantarea unei structuri politice alternative care să poată prelua conducerea statului algerian. Dacă în Algeria a contat – ca și după Primăvara Arabă, în Egipt – relevanța și locul forțelor armate în societate, în Liban, implozia politică nu are alternativă astăzi decât în această perspectivă a nașterii unei elite politice alternative.

Însă, trebuie spus că alegerile anticipate nu sunt o soluție decât de moment. Mânia publică și oprobiul asupra întregii clase politice nu pot să mai fie oprite în prezent, după ce abia au fost gestionate în octombrie 2019. Populația pornită împotriva întregii clase politice nu mai acceptă formule paleative, ca cele ale alegerilor anticipate cu obligativitatea de a alege între aceiași actori. Nici măcar schimbarea figurilor din prim-plan nu mai e acceptabilă.

Premierul Hassan Diab a recunoscut criza structurală a clasei politice și nevoia schimbării Parlamentului, dar s-a oprit aici. Nu a văzut că o clasă politică alcătuită din partidele politice religioase și sectare, că grupările paramilitare și opțiunile finanțării oligarhice de până acum, nu mai pot supraviețui. Iar un guvern dat de

alegeri între aceiași actori va duce la un alt nou eșec cât de curând. Sperăm nu și la o nouă criză, explozie, accident industrial tehnologic sau catastrofă determinate de lipsa capacității politice și administrative, probate deja la 4 august a.c. de actuala clasă politică libaneză.

„Cernobîlul libanez” și efectele de stat slab sau eșuat în Orientul Mijlociu²⁹

Conceptul de „stat slab” este unul disputat și acceptat și doar în mica măsură controversat. Astfel, elementele care pun în discuție capacitatea și gradul de seriozitate și funcționalitate a unui stat, care poate fi calificat drept stat puternic și serios, stat cu toate atribuțiile sau stat slab se definesc în funcție de câteva caracteristici. Barry Buzan folosește cele trei caracteristici fundamentale³⁰:

- ideea coezivă ce dă naștere unui stat și care unește societatea, populația și generații succesive (conține legitimitatea, credibilitatea, elementele de substanțiere a statului);
- expresia fizică a unui stat – teritoriu, populație, autoritate asupra acestora de către o conducere recunoscută și respectată;
- instituționalizarea ca stat – respectiv crearea sistemului instituțional prin intermediul căruia se poate exercita autoritatea în stat și cetățeanul poate interacționa și se poate simți protejat de către stat, iar conducătorul poate fi ales legitim, inclusiv componenta prin care fiecare cetățean al statului poate ocupa o funcție relevantă în stat și poate influența deciziile în acel stat.

Max Weber adaugă autoritatea impersonală condusă de legislație, respectiv componenta concretă de suveranitate în sensul existenței, manifestării, recunoașterii suveranității de către puterea în stat și a exercitării acesteia neîngrădit decât de lege și regulile fondatoare ale statului – Constituția sau actul constitutiv³¹. Aici ar putea intra capacitatea administrativă și îndeplinirea rolului de asigurare a serviciilor față de cetățean și a respectării angajamentelor față de partenerii similari, statele, la nivel internațional.

Statul eșuat, statul fragil sau colapsul statului sunt elementele extreme ale statului slab. Sunt concepte introduse de către The Fund for Peace,

organizație neguvernamentală americană care și asigură evaluarea statelor slabe și eșuate utilizând un indice al fragilității statelor³².

Principalele caracteristici ale statului eșuat ar fi:

- neîndeplinirea principalelor condiții de funcționare și responsabilități;
- lipsa unui guvern suveran funcțional;
- pierderea legitimității, precum și lipsa funcționalității oricărui guvern și lipsa de credibilitate a întregii clase politice.

Pentru The Fund for Peace, criteriile statului eșuat ar fi³³:

- lipsa controlului asupra teritoriului;
- pierderea monopolului utilizării legitime a forței fizice;
- eroziunea autorității legitime să ia decizii colective;
- incapacitatea de a oferi servicii publice;
- incapacitatea de a interacționa cu alte state, ca membru deplin al comunității internaționale.

După toate aceste criterii, Libanul a fost întotdeauna un stat slab, iar deflagrația din 4 august a.c. expune condiții suficiente pentru a fi calificat drept stat eșuat.

Israelul, care a avut confruntări directe cu Libanul, cu care nu are legături diplomatice, ar putea fi cel mai afectat de prezența unei cantități uriașe de precursor al explozibililor – azotatul de amoniu – la Beirut, păstrat în condiții improprii. Produsul a fost utilizat deja în Oklohama pentru un atac terorist. În cazul transferurilor de arme dintre Iran și Hezbollahul libanez, statul israelian le urmărește și le elimină chirurgical în Siria³⁴.

Autoritățile israeliene știau despre cantitatea de azotat de amoniu. Cum ar ști și despre cantități de arme care s-ar vinde către Hezbollah sau care s-ar afla în depozite secrete ale Hezbollah-ului libanez. Cum ar trebui să reacționeze? Este acest tip de prezență o țintă legitimă pe teritoriul Libanului? Dacă e să luăm în considerare acțiunile din Siria, orice transfer de rachete sau arme care permite atacarea de către Hezbollah-ul cantonat în sudul Libanului a localităților din Israel e considerat o țintă legitimă. Dar prezența unei asemenea amenințări în Beirut ar putea să fie o asemenea opțiune? Să fie considerat o amenințare similară?

Această dilemă nu ar fi putut interveni în mod real, chiar dacă evaluarea sa e necesară în planificarea strategică, așa cum am schițat-o deja. Cu certitudine, Israelul ar fi găsit canalele de comunicare pentru a transmite Libanului, prin intermediari care ar fi fost ascultați, că are o problemă în legătură cu depozitul, încărcătura, armamentele din depozitul din Beirut, cu modul în care sunt păstrate și administrate. Cu certitudine ar fi comunicat solicitarea imperativă ca guvernul libanez să facă ordine (în acești peste șase ani) și să elimine o asemenea amenințare, o bombă cu ceas la adresa propriei populații și, nu în ultimul rând, la adresa Israelului.

De asemenea, admitând că nu ar fi fost ascultat, sigur un stat serios și respectabil nu ar fi declanșat niciodată un atac, chiar acoperit de negarea credibilă, asupra depozitului, știind efectele unei asemenea explozii catastrofale. În plus, nu poți ascunde nimic astăzi, în era digitală, în cazuri majore, față de serviciile de informații puternice ale lumii, în orice colț al lumii te-ai afla. Israelul ar fi găsit elemente și acțiuni intermediare, nuanțate, pentru a expune public existența acestui pericol major, pentru a blama conducerea libaneză care nu ține cont de responsabilitățile sale și care-și pune în pericol întreaga populație.

Totuși dilema subzistă, iar existența reacțiilor nuanțate ale unui stat responsabil, cu respectabilitate pe scena internațională, nu poate acoperi și ține sub tăcere, în cazul conflictului de valori fundamentale, amenințarea pe care o reprezintă un stat slab sau eșuat³⁵. Pentru că lipsa capacității administrative, problemele de credibilitate și legitimitate ale clasei politice, incapacitatea de a gestiona un pericol despre care știa întreaga administrație ani la rând subliniază, de fapt, situația unui stat slab, care nu-și poate purta singur de grijă. Sau a cărei clasă politică nu e în stare să gestioneze cele mai vizibile și mai grave probleme pentru siguranța propriei populații.

Aranjamente inacceptabile și crizele secundare în conflictele prelungite: Israel, Bosnia și Herzegovina, Irak, Siria

Situația statului eșuat Liban ridică semne de întrebare majore pe numeroase alte aranjamente post-război. Mai întâi, până la acordul Israel –

Emiratele Arabe Unite, care a exclus declararea de către premierul Benjamin Netanyahu a suveranității israeliene asupra unor teritorii din Cisiordania³⁶, inițierea unor acte unilaterale impuse putea crea aranjamente inacceptabile, care urmau să se răzbine în timp. Orientul Mijlociu și dosarul aferent constituie o asemenea ilustrare, inclusiv prin Acordul de Pace de la Oslo (1993), cu premiile Nobel pentru Pace acordate în 1994 pentru Yasser Arafat, Shimon Perez și Itzak Rabin; un acord care a fost, de asemenea, inacceptabil cel puțin unei părți a populației israeliene, având ca rezultat asasinarea premierului israelian în funcție, Itzak Rabin, la 4 noiembrie 1995, de către ultranaționalistul evreu Yigal Amir, și relansarea Intifadei.

În Bosnia și Herzegovina, Acordul de la Dayton, semnat la 1 noiembrie 1995, a creat premisele împărțirii puterii între comunitățile sârbă, croată și bosniacă (sârbo-croați trecuți la religia musulmană) în cel mai sângeros conflict din Balcanii de Vest. Astfel, noul stat confederativ Bosnia și Herzegovina a fost creat din două entități, Republica Srpska și Federația Bosnia-Herzegovina (croato-musulmană), având la conducere o formulă trilaterală de președinție rotativă în care fiecare președinte deține mandatul câte opt luni, având primul rol de două ori timp de patru ani³⁷. Și aici, acordurile au soluționat conflictul, dar efectele în timp se manifestă și astăzi, cu impact negativ.

Cel mai clar exemplu este Cazul Sejdic – Finci, judecat la CEDO³⁸. Ambii născuți și crescuți în Sarajevo, în perioada fostei Iugoslavii, cei doi cetățeni ai Bosniei și Herzegovina sunt, primul, de origine romă și al doilea de religie evreiască și ambii au câștigat, într-un caz comun soluționat de Marea Cameră, la 22 decembrie 2009, împotriva statului Bosnia și Herzegovina. Motivul a fost discriminarea pe criterii etnice și religioase și imposibilitatea ca cei doi să poată fi aleși vreodată ca președinți ai statului în care trăiau. Pe baza Convenției pentru Drepturile Omului și apartenenței Bosniei și Herzegovina la Consiliul Europei, cazul a subliniat imposibilitatea ca regulile democratice să fie aplicate în cazul aranjamentului din acest stat.

Astfel că, pentru a înainta în drumul său de integrare în NATO și UE, pentru a valida regulile democratice aplicabile tuturor cetățenilor săi,

Bosnia și Herțegovina trebuie, în prezent, să modifice aceste aranjamente și să devină un stat democratic autentic. În cazul său, nu s-a pus problema izbucnirii unei crize directe, fiind vorba despre un stat european și cu legături strânse cu democrațiile consacrate din Europa. Totuși, pronunțarea CEDO relevă faptul că și capacitatea statului bosniac de a-și îndeplini atribuțiile ar putea fi pusă sub semnul întrebării.

Și în cazul Irakului, epoca post-Sadam Hussein a adus condiționări de aceeași factură, de împărțire a puterii pe baze sectare și etnice³⁹. Aici, cele trei componente care alcătuiesc statul irakian sunt kurzii sunniți din nord-vest, cu autonomie proprie, arabii sunniți și cei șiiți. Saddam Hussein a fost sunnit și a organizat un stat Baas Arab Socialist, în care sunniții dețineau funcțiile de conducere, fiind supra-reprezențați în aparatul militar și de intelligence, reprimând atât kurzii, cât și șiiții. S-a mers până la atacul chimic de la Halabja împotriva kurzilor, la 16 martie 1988, parte a campaniei Anfāl care a ucis între 50.000 și 182.000 de kurzi și asirieni între 1986-1989. De asemenea, gazul sarin a fost folosit împotriva șiiților în 1991, în timpul unei revolte care a dus la cucerirea localității Karbala de către șiiți⁴⁰.

Aranjamentul numit al Muhasasa – para-normativ, neinclus în Constituția din 2005, dar în contextul acesteia – prevede numirea politicianilor pe baza identității lor etnice și sectare, nu pe baza ideilor politice, a ideologiei, meritelor sau competenței⁴¹. Modelul libanez s-a aplicat și aici, prin aranjamente de împărțire a funcțiilor politice de vârf la nivel executiv între principalele grupuri etno-sectare din Irak, respectiv sunniți, șiiți și kurzi, plus alte minorități. Președintele statului, președintele Parlamentului și primul ministru sunt respectiv un kurd, un sunnit și un șiiit. În rest, aranjamentele se fac pe această bază și pe procente deținute la vot și în Parlament între diferitele partide, împingând spre un sistem partitocratic mai degrabă decât democratic. Contestările nu au lipsit, iar în marile manifestații împotriva guvernului, de la sfârșitul anului 2019, mase de manifestanți trans-sectari și pan-religii au contestat guvernul, indiferent de apartenența religioasă, arătând falimentul aranjamentelor și clasei politice irakiene post-Saddam Hussein.

Perspectiva modelului libanez, respectiv irakian, amenință să se repete în Siria, după o eventuală încheiere a războiului civil. Dincolo de influențele internaționale în Siria, o formulă de împărțire a puterii politice va trebui să țină cont de demografie și cetățenie, în condițiile în care sistemul dominant allawit al lui Bashar al Assad, în care minoritatea reprezentând o sectă șiiită domină majoritatea sunnită, alcătuită de triburi turcomane, arabe, dar și de druzi și creștini maroniți, nu are cum să mai supraviețuiască. Prin urmare, o formulă tip Liban ar putea să se repete, însă ea creează, în timp, probleme majore de credibilitate prin faptul că osifică atașamente sectare în detrimentul coeziunii statale și permite alocări de funcții pe alte criterii decât cele democratice, meritocratice și de legitimitate.

Și aceasta ar trebui să fie o lecție învățată a deflagrației catastrofale care a devastat Beirutul: aranjamentele de împărțire a puterii post-conflict nu trebuie menținute în timp, ci tot regulile democratice și formulele partidelor multietnice ar trebui să devină dominante. În caz contrar, apar probleme majore de coeziune socială și osificare a feodelor sectare, aceste adevărate monarhii sectare și monopoluri asupra comunităților regăsite în statele slabe, și care subminează orice posibilitate de constituire a unui stat modern, funcțional, serios.

Bibliografie:

1. KRAYEM Hassan, *The Lebanese Civil War and the Taif Agreement*, American University of Beirut, 10 iunie 2012, la <https://abdallah.hiof.no/projects/pspa/conflict-resolution.html>.
2. YEUNG Jessie, Luke McGee, *What we know about the Beirut blast*, CNN, August 6, 2020, Updated 1102 GMT, la <https://edition.cnn.com/2020/08/05/middleeast/beirut-blast-explainer-intl-hnk/index.html>.
3. Documentele Curții de Justiție despre confiscarea încărcăturii de azotat de amoniu a navei, văzute de CNN, Idem. Steven A. COOK, *The only political system the country has ever known is collapsing, and it's never coming back*, Foreign Policy, 30 July 2020, la <https://foreignpolicy.com/2020/07/30/lebanon-as-we-know-it-is-dying/>.

4. REGENCIA Ted, Linah Alsaafin & Ramy Allahoum, *Endemic corruption caused Beirut blast, says Diab: Live updates*, Al Jazeera, 11 Aug 2020, la <https://www.aljazeera.com/news/2020/08/beirut-police-fire-tear-gas-protesters-regroup-live-updates-200810010528285.html>.
5. MYERS Denys P., *The Mandate System of the League of Nations*, în *The Annals of the American Academy of Political and Social Science*, Nr. 96, 1 Ianuarie 1921.
6. National Council of Arab Americans (NCA), *Historical Chronology of Lebanon*, 19 martie 2009, la https://web.archive.org/web/20090319121339/http://www.arab-american.net/Historical_Chronology_of_Lebanon.pdf.
7. BRUNET-JAILLY Emmanuel, *Border Disputes: A Global Encyclopedia* (3 vol): A Global Encyclopedia, ABC-CLIO, ISBN 978-1-61969-024-9, 2015.
8. JOHNSTONE, Patrick, Miller Douane Alexander, *Believers in Christ from a Muslim Background: A Global Census*, *Interdisciplinary Journal of Research on Religion*, nr. 11 din 2015, p. 16, la https://www.academia.edu/16338087/Believers_in_Christ_from_a_Muslim_Background_A_Global_Census.
9. INHORN, Marcia C., Soraya Trmayne, *Islam and Assisted Reproductive Technologies*, 2012.
10. DE CLERCK Dima, *Ex-Militia fighters in post-war Lebanon*, în *Reconciliation, reform and resilience: positive peace for Lebanon*, ACCORD, at https://web.archive.org/web/20150923200854/http://www.c-r.org/sites/c-r.org/files/accord24_ExMilitiaFighters.pdf.
11. LESSA Francesca, Olsen Tricia D, Payne Leigh A, Pereira Garbiel, Reiter Andrew G, *Persistent or Eroding Impunity? The Divergent Effects of Legal Challenges to Amnesty Laws for Past Human Rights Violations*, *Israel Law Review*, nr 47(1), 2014.
12. CHIFU Iulian, *Costurile responsabilității în criză: Implozia sistemului politic libanez*, în *Adevărul*, 10 august 2020, la https://adevarul.ro/international/in-lume/costurile-responsabilitatii-incriza-implozia-sistemului-politic-libanez-1_5f300e545163ec4271d0b6c1/index.html.
13. KATERJI Oz, *The Beirut Blast Is Lebanon's Chernobyl*, *Foreign Policy*, 5 august 2020, la <https://foreignpolicy.com/2020/08/05/beirut-explosion-blast-lebanon-ammonium-nitrate-chernobyl-corruption/>.
14. Report Syndication, *Lebanon Protesters Found Strength in Unity, Ditched Sectarianism*, 27 octombrie 2019, la <https://reportsyndication.news.blog/2019/10/27/lebanon-protesters-find-strength-in-unity-ditched-sectarianism/>.
15. USA Today, *Lebanon president: Beirut explosion either due to negligence or missile, bomb*, Aug 7, 2020, la <https://eu.usatoday.com/story/news/world/2020/08/07/beirut-explosion-due-negligence-missile-says-lebanon-president/3317722001/>.
16. URAS Umut&Farah Najjar, *Clashes in Beirut as anger swells over port blast: Live updates*, AL Jazeera, 9 august 2020, la <https://www.aljazeera.com/news/2020/08/60-missing-beirut-mega-blast-live-updates-200808061240497.html>.
17. QIBLAWI Tamara, Ali Younes, Mostafa Salem and Ghazi Balkiz, *Lebanon's government steps down in wake of Beirut blast*, CNN, 11 august 2020, la <https://edition.cnn.com/2020/08/10/middleeast/lebanon-government-future-intl/index.html>.
18. ANDERSON Becky, *Lebanon has always deserved better from its leaders. The port blast lays that bare*, CNN, August 9, 2020, la <https://edition.cnn.com/2020/08/09/opinions/beirut-blast-anderson-opinion-intl/index.html>.
19. CHIFU Iulian, *Cernobilul libanez: „Casus Beli” versus „Țintă legitimă” pentru Israel*, în *Adevărul*, 11 august 2020, la https://adevarul.ro/international/in-lume/cernobilul-libanez-casus-beli-versus-Tinta-legitima-israel-1_5f3180e55163ec4271d8a9c9/index.html.
20. BUZAN Barry, *Popoarele, Statele și Frica*, Editura Cartier, Chișinău, 2014, ISBN 978-9975-79-727-6, 385 p.
21. LINZ Juan J., Stephan Alfred, *Problems of democratic transition and consolidation*, 1996.
22. Fund for Peace, *Fragile State Index*, <https://fragilestatesindex.org/>.
23. Fund for Peace, *What Does Fragility Means?*, la <https://web.archive.org/web/20150104202014/http://ffp.statesindex.org/faq-06-state-fragility>.

24. Times of Israel, *IDF official said to confirm attack in Syria: 'First strike on Iranian targets'*, 16 aprilie 2019, la <https://www.timesofisrael.com/idf-official-confirms-attack-in-syria-first-strike-on-live-iranian-targets/>.
25. Maritime Terrorism Resource Portal, *Seafarer Rights, Ship Abandonment, and the Explosion in Beirut*, 5.06.2020, la <https://stableseas.org/blue-economy/explosion-beirut-seafarer-rights>.
26. BAKER Peter, Isabel Kershner, David D. Kirkpatrick and Ronen Bergman, *Israel and United Arab Emirates Strike Major Diplomatic Agreement*, The New York Times, 13 august 2020, la <https://www.nytimes.com/2020/08/13/us/politics/trump-israel-united-arab-emirates-uae.html>.
27. ALBRIGHT Madeleine, *Letter Dated 29 November 1995 from the Permanent Representative of the United States of America to the United Nations Addressed to the Secretary General*, UN, la https://peacemaker.un.org/sites/peacemaker.un.org/files/BA_951121_DaytonAgreement.pdf.
28. ECHR, Press Release, *Grand Chamber judgment, Sejdic and Finci v. Bosnia and Herzegovina (application nos.27996/06 and 34836/06)*, 22.12.2009, la <https://hudoc.echr.coe.int/eng-press#%7B%22itemid%22:%5B%222003-2974573-3281658%22%5D%7D>.
29. HAMZEH al-Shadeedi, Erwin van Veen, *Iraq's Adolescent Democracy*, Clingendael, June 2020, at <https://www.clingendael.org/pub/2020/iraqs-adolescent-democracy/>.
30. NGUYEN Michael, *Report Confirms Iraq Used Sarin in 1991*, Arms Control Association, <https://www.armscontrol.org/act/2006-01/report-confirms-iraq-used-sarin-1991>.
31. MORADI Fazil, *The Force of Writing in Genocide: On Sexual Violence in the Al Anfal Operations and Beyond*, in *Gender Violence in Peace and War: States of Complicity*, New Brunswick, NJ and London: Rutgers University Press.
32. ARWA Ibrahim, *Muhasasa, the political system reviled by Iraqi protesters*, Al Jazeera, 4 decembrie 2019, la <https://www.aljazeera.com/news/2019/12/muhasasa-political-system-reviled-iraqi-protesters-191202201939755.html>.

¹ Acordurile de la Taif, 22 octombrie 1989 – Acordul de Reconciliere Națională. Vezi Krayem Hassan, *The Lebanese Civil War and the Taif Agreement*, American University of Beirut, 10 iunie 2012, la <https://abdallah.hiof.no/projects/pspa/conflict-resolution.html>.

² Jessie Yeung, Luke McGee, *What we know about the Beirut blast*, CNN, August 6, 2020, Updated 1102 GMT, la <https://edition.cnn.com/2020/08/05/middleeast/beirut-blast-explainer-intl-hnk/index.html>.

³ Documentele Curții de Justiție despre confiscarea încărcăturii de azotat de amoniu a navei, văzute de CNN; Idem. Steven A. Cook, *The only political system the country has ever known is collapsing, and it's never coming back*, Foreign Policy, 30 July 2020, la <https://foreignpolicy.com/2020/07/30/lebanon-as-we-know-it-is-dying/>.

⁴ Ted Regencia, Linah Alsaafin & Ramy Allahoum, *Endemic corruption caused Beirut blast, says Diab: Live updates*, Al Jazeera, 11 Aug 2020, la <https://www.aljazeera.com/news/2020/08/beirut-police-fire-tear-gas-protesters-regroup-live-updates-200810010528285.html>.

⁵ Denys P. Myers, *The Mandate System of the League of Nations*, în *The Annals of the American Academy of Political and Social Science*, Nr. 96, 1 Ianuarie 1921, pp74-77.

⁶ National Council of Arab Americans (NCA), *Historical Chronology of Lebanon*, 19 martie 2009, la https://web.archive.org/web/20090319121339/http://www.arab-american.net/Historical_Chronology_of_Lebanon.pdf.

⁷ Emmanuel Brunet-Jailly, *Border Disputes: A Global Encyclopedia* (3 vol.): A Global Encyclopedia, ABC-CLIO, ISBN 978-1-61969-024-9, 2015, pp. 353 și următoarele.

⁸ Patrick Johnstone, Miller Douane Alexander, *Believers in Christ from a Muslim Background: A Global Census*, *Interdisciplinary Journal of Research on Religion*, nr. 11 din 2015, p. 16, la https://www.academia.edu/16338087/Believers_in_Christ_from_a_Muslim_Background_A_Global_Census.

⁹ Steven A. Cook, *Op.cit.*

¹⁰ Patrick Johnstone, Alexander Miller Duane, *Op.cit.*

¹¹ Marcia C. Inhorn, Soraya Tremayne, *Islam and Assisted Reproductive Technologies*, 2012, p.238.

- ¹² Dima de Clerck, *Ex-Militia fighters in post-war Lebanon*, in *Reconciliation, reform and resilience: positive peace for Lebanon*, ACCORD, pp. 23-24 at https://web.archive.org/web/20150923200854/http://www.c-r.org/sites/c-r.org/files/accord24_ExMilitiaFighters.pdf.
- ¹³ Francesca Lessa, Olsen, Tricia D, Payne, Leigh A, Pereira Garbiel, Reiter Andrew G, *Persistent or Eroding Impunity? The Divergent Effects of Legal Challenges to Amnesty Laws for Past Human Rights Violations*, Israel Law Review, nr 47(1), 2014, pp. 105-106.
- ¹⁴ Vezi Iulian Chifu, *Costurile responsabilității în criză: Implozia sistemului politic libanez*, în *Adevărul*, 10 august 2020, la https://adevarul.ro/international/in-lume/costurile-responsabilitatii-incriza-implozia-sistemului-politic-libanez-1_5f300e545163ec4271d0b6c1/index.html.
- ¹⁵ Jessie Yeung, Luke McGee, *Op.cit.*
- ¹⁶ Oz Katerji, *The Beirut Blast Is Lebanon's Chernobyl*, Foreign Policy, 5 august 2020, la <https://foreignpolicy.com/2020/08/05/beirut-explosion-blast-lebanon-ammonium-nitrate-chemobyl-corruption/>.
- ¹⁷ Report Syndication, *Lebanon Protesters Found Strength in Unity, Ditched Sectarianism*, 27 octombrie 2019, la <https://reportsyndication.news.blog/2019/10/27/lebanon-protesters-find-strength-in-unity-ditched-sectarianism/>.
- ¹⁸ *Idem.*
- ¹⁹ Oz Katerji, *Op.cit.*
- ²⁰ USA Today, *Lebanon president: Beirut explosion either due to negligence or missile bomb*.
- ²¹ *Idem.*
- ²² Umut Uras & Farah Najjar, *Clashes in Beirut as anger swells over port blast: Live updates*, AL Jazeera, 9 august 2020, la <https://www.aljazeera.com/news/2020/08/60-missing-beirut-mega-blast-live-updates-200808061240497.html>.
- ²³ Tamara Qiblawi, Ali Younes, Mostafa Salem and Ghazi Balkiz, *Lebanon's government steps down in wake of Beirut blast*, CNN, 11 august 2020, la <https://edition.cnn.com/2020/08/10/middleeast/lebanon-government-future-intl/index.html>.
- ²⁴ Vezi Iulian Chifu, *Costurile responsabilității în criză: Implozia sistemului politic libanez*.
- ²⁵ Becky Anderson, *Lebanon has always deserved better from its leaders. The port blast lays that bare*, CNN, August 9, 2020, la <https://edition.cnn.com/2020/08/09/opinions/beirut-blast-anderson-opinion-intl/index.html>.
- ²⁶ Ted Regencia et al, *Op.cit.*
- ²⁷ Becky Anderson, *Op.cit.*
- ²⁸ Steven A Cook, *Op.cit.*
- ²⁹ Iulian Chifu, *Cernobilul libanez: „Casus Beli” versus „Țintă legitimă” pentru Israel*, în *Adevărul*, 11 august 2020, la https://adevarul.ro/international/in-lume/cernobilul-libanez-casus-beli-versus-Tinta-legitima-israel-1_5f3180e55163ec4271d8a9c9/index.html.
- ³⁰ Barry Buzan, *Popoarele, Statele și Frica*, Editura Cartier, Chișinău, 2014, ISBN 978-9975-79-727-6, 385 p.
- ³¹ Juan J. Linz, Stephan Alfred, *Problems of democratic transition and consolidation*, 1996, p.17.
- ³² Fund for Peace, *Fragile State Index*, <https://fragilestatesindex.org/>.
- ³³ *Idem*; Vezi și Fund for Peace, *What Does Fragility Means?*, la <https://web.archive.org/web/20150104202014/http://ffp.statesindex.org/faq-06-state-fragility>.
- ³⁴ Times of Israel, *IDF official said to confirm attack in Syria: 'First strike on Iranian targets'*, 16 aprilie 2019, la <https://www.timesofisrael.com/idf-official-confirms-attack-in-syria-first-strike-on-live-iranian-targets/>.
- ³⁵ Maritime Terrorism Resource Portal, *Seafarer Rights, Ship Abandonment, and the Explosion in Beirut*, 5.06.2020, la <https://stableseas.org/blue-economy/explosion-beirut-seafarer-rights>.
- ³⁶ Peter Baker, Isabel Kershner, David D. Kirkpatrick and Ronen Bergman, *Israel and United Arab Emirates Strike Major Diplomatic Agreement*, The New York Times, 13 august 2020, la <https://www.nytimes.com/2020/08/13/us/politics/trump-israel-united-arab-emirates-uae.html>.
- ³⁷ Madeleine Albright, *Letter Dated 29 November 1995 from the Permanent Representative of the United States of America to the United Nations Addressed to the Secretary General*, UN, la https://peacemaker.un.org/sites/peacemaker.un.org/files/BA_951121_DaytonAgreement.pdf.
- ³⁸ ECHR, Press Release, *Grand Chamber judgment, Sejdic and Finci v. Bosnia and Herzegovina (application nos. 27996/06 and 34836/06)*, 22.12.2009, la <https://hudoc.echr.coe.int/eng-press#%7B%22itemid%22:%5B%22003-2974573-3281658%22%5D%7D>.
- ³⁹ Hamzeh al-Shadeedi, Erwin van Veen, *Iraq's Adolescent Democracy*, Clingendael, June 2020, at <https://www.clingendael.org/pub/2020/iraqs-adolescent-democracy/>.
- ⁴⁰ Michael Nguyen, *Report Confirms Iraq Used Sarin in 1991*, Arms Control Association, <https://www.armscontrol.org/act/2006-01/report-confirms-iraq-used-sarin-1991>; Fazil Moradi, *The Force of Writing in Genocide: On Sexual Violence in the Al Anfal Operations and Beyond*, in *Gender Violence, in Peace and War: States of Complicity*, New Brunswick, NJ and London: Rutgers University Press, pp 102-115.
- ⁴¹ Arwa Ibrahim, *Muhasasa, the political system reviled by Iraqi protesters*, Al Jazeera, 4 decembrie 2019, la <https://www.aljazeera.com/news/2019/12/muhasasa-political-system-reviled-iraqi-protesters-191202201939755.html>.

COORDONATELE RĂZBOIULUI DE GENERAȚIA A CINCEA

Daniel COCOLICI*
Sorinel POPESCU

Abstract

The transformation of the global security surprises in most of the cases the military organizations structured based on the rules of the last major war they fought, so is paramount to observe early a shift in paradigm in order to have the necessary time to adapt.

The type of military confrontation known today as the hybrid war, can be a model on how the nature of the war is changing, but the new generation of war will probably surpass it both in amplitude and complexity.

The fifth generation of war will probably absorb some of the characteristics of the previous generations of war, mainly the asymmetry and maneuvering, extended across multiple domains, with the effects of the confrontation rippling beyond the domain limits. The military factor will maintain its importance in the economy of forces and means employed, but it cannot remain isolated from the other factors anymore.

Although the military confrontation will include more and more non-state entities, the fifth generation war will remain the reflection of the renewed global power competition between the states. It is to be expected that it will manifest itself along the demarcation lines of the areas of influence of the states and states alliances, contributing to their shaping. Most likely, despite the confrontation, the state actors will desire to keep the illusion of peace to invalidate the legal base of the employment of the armed forces. The aggressor state will perform the strategic modeling initially aiming the political and social system of the target state to induce discontent among the people, following with efforts on the international arena to gain legitimacy.

Keywords: *fifth generation war, global security, warfare, strategy.*

Context

Caracterul războiului, ca fenomen social complex, s-a transformat în paralel și intrinsec odată cu evoluția societății umane, fiind influențat de fizionomia conflictualității individuale, sociale, economice, politice și militare de la un moment dat. Războaiele au reflectat stadiul de dezvoltare atins de societatea umană, precum și modul în care aceasta percepe amenințările și riscurile. Fără îndoială, războiul a avut și are un caracter distructiv, dar, în multe situații, a reprezentat și un punct de plecare în dezvoltarea societăților. Realizările tehnologice influențează la rândul lor fizionomia războiului, tot așa cum organizarea sistemului de relații internaționale și percepția

decidenților politici față de legitimitatea acțiunilor distructive caracteristice luptei armate, ca forma de violență asumată, își pun amprenta asupra inițierii, ducerii și finalizării acțiunilor militare.

În ultimele patru secole dezvoltarea armatelor a urmat dezvoltarea societăților, beneficiind de progresele tehnologice și industriale înregistrate de acestea. Organizațiile militare învață din experiențele câștigate în confruntările la care sunt supuse, dar caută, teoretic, și să se adapteze în permanență la percepția amenințărilor de securitate curente, ca formă de identificare a noilor forme de conflict. De regulă, transformarea este una lentă și poate traversa perioade extinse de stagnare, asociate perioadelor de pace în care resursele

**Autorii sunt experți în cadrul Ministerului Apărării Naționale.*

societății sunt direcționate pentru satisfacerea nevoilor sociale imediate. Sunt necesare perioade lungi de timp pentru a organiza, echipa și instrui o armată, cu scopul de a o pregăti să răspundă eficient la războiul viitorului. În realitate, armatele sunt birocratii inerțiale, ceea ce le face dificil de transformat. Transformarea mediului de securitate surprinde de cele mai multe ori armatele organizate după regulile ultimului război major pe care l-au purtat, motiv pentru care este necesar ca schimbarea paradigmei să fie observată din timp, pentru a beneficia de răgazul necesar adaptării.

Conform multor autori contemporani, la acest moment se constată o „diminuare a riscului confruntării armate, ceea ce a făcut ca războiul să nu mai implice cucerirea de teritorii, ci a conștiinței populațiilor din teritoriile/stările țintă. Geografia fizică a rămas importantă pentru teritoriile care pot alimenta războiul cu resurse naturale (energetice, alimentare) sau care prezintă relevanță strategică. În schimb, geografia umană a devenit noul câmp de luptă al războiului, în condițiile în care noua tehnologie poate influența decizia unui stat și chiar comportamentul unei societăți”¹.

Războiul „a dobândit un pronunțat caracter informațional, întrucât vizează manipularea unui stat și a cetățenilor săi. Acțiunile lui se derulează exploatând, în special, dimensiunea virtuală creată de noua tehnologie. Internetul favorizează circulația rapidă și masivă a informației, accelerând procesul de globalizare. Dar facilitățile acestui canal de comunicare sunt exploatate și pentru lansarea unor ample operații subversive. Internetul asigură camuflarea atacului informațional, îi imprimă caracter global și permite să fie executat cu precizie, de la distanță și fără riscuri”².

Un model generațional de descriere a modului în care este abordată problematica războiului poate fi util pentru a sesiza parametrii schimbărilor de paradigmă înregistrați de-a lungul timpului. Punctul de plecare al acestei abordări îl poate constitui momentul Păcii de la Westfalia, ca origine a principiilor esențiale pentru relațiile internaționale moderne, inclusiv inviolabilitatea frontierelor și neamestecul în afacerile interne ale statelor suverane³. Această abordare permite o bună reprezentare a relației stabilite între sistemul

de relații internaționale al timpului, dezvoltarea societății, dezvoltarea tehnologică și practica războiului, constituind totodată o bază de plecare corectă pentru o proiecție în viitor.

Războaiele din generațiile I-III

Primele trei generații ale războiului – **războiul clasic, războiul de uzură și războiul manevrier** – constituie etape distincte în transformarea războiului în epoca post-Westfalia, trecerea de la un tip de confruntare armată la alta suprapunându-se schimbării principiilor de organizare a sistemelor de relații internaționale succesive: de la confruntarea dintre marile puteri la Concertul Europei, formarea Ligii Națiunilor și apariția Organizației Națiunilor Unite. Toate cele trei generații reflectă modul în care organizarea economică a societăților a putut fi pusă în sprijinul interacțiunii militare, pe baze agrare, industriale sau post-industriale; și toate trei au exploatat la maximum gradul de dezvoltare industrială și tehnologică la nivelul realității câmpului de luptă. Primele trei generații de război luau în calcul statele și alianțele drept principali actori implicați în confruntare, în perioade în care războiul constituia o formă acceptabilă a finalizării competiției interstatale. În egală măsură, în toate cele trei situații, distincția dintre civili și militari era bine definită, chiar dacă pe măsura tranzitului generațional nevoia de a spori numărul de militari a determinat, în situații extreme, înrolări din ce în ce mai extinse.

Războaiele din primele trei generații urmau un algoritm bine definit constând din trei etape distincte. În timp, durata, amplitudinea și complexitatea acțiunilor specifice fiecăreia, precum și intensitatea acestora au variat în funcție de dezvoltările tehnologice, scopurile urmărite, timpul de atingere a obiectivelor etc. În general, prima etapă a constat în: pregătirea operațiilor din timp de pace desfășurate la nivel național și internațional – modelarea strategică: realizarea unor noi aranjamente de securitate, crearea unei legitimități la nivel internațional care să justifice acțiunile ulterioare, pregătirea populației proprii, dar și a opiniei publice internaționale pentru război. Pe timpul acestei faze erau mobilizate resursele naționale (materiale, financiare,

umane, informaționale etc.) și executate operații subversive (cercetare, spionaj, sabotaj) împotriva statului țintă. Ce-a de-a doua etapă consta în desfășurarea propriu-zisă a războiului, inclusiv confruntarea militară în sine, iar cea de-a treia era reprezentată de negocierile de pace prin care se redeseau sferile de influență. În perioada de după cel de-al Doilea Război Mondial, perioada post-conflict a inclus operațiile de stabilizare și sprijin, care în ultimele războaie (Afganistan și Irak) au depășit cu mult perioadele alocate primelor două faze ale conflictului.

Războiul de primă generație (războiul clasic între state naționale).

Războiul din prima generație a apărut la mijlocul secolului al XVII-lea, constituind forma clasică a războaielor dintre state naționale și care a culminat cu războaiele napoleoniene. Confruntarea armată se baza pe utilizarea armelor de foc cu încărcare manuală, trupe semnificative numeric, un sistem de înrolare obligatorie și poziționări ale formației pentru maximizarea puterii de foc în scopul compensării limitelor armamentului avut la dispoziție. Era liniar în natură, deoarece a permis ca volumul maxim de foc să fie concentrat asupra inamicului într-o confruntare caracterizată de disciplină. Liniarizarea caracteriza atât ofensiva, cât și defensivă, în apărare existând conceptul menținerii liniei frontului, o reflecție a obsesiei statului național pentru control teritorial, în detrimentul manevrei. Această generație a creat o cultură a ordinii militare la nivelul existent anterior în legiunile Imperiului Roman. În timp ce strategia se baza pe acțiuni de masă, tactica a fost centrată pe acțiuni în linie și coloană, pentru maximizarea puterii de foc⁴.

Este de remarcat faptul că acest mod de confruntare avea un caracter formal, fiind precedat de o declarație de război, iar semnarea apartenenței militarilor la fiecare dintre tabere se făcea prin portul uniformei respective.

Războiul de generația a doua (războiul de uzură)

Războiul de a doua generație a fost influențat decisiv de noile tehnologii apărute în secolul XIX. Aceste tehnologii au sporit puterea de foc a armamentului de infanterie, prin apariția

mitralierelor și puștilor cu încărcare automată și prin introducerea pe câmpul de luptă a focului distrugător al artileriei. Scopul luptei îl constituia eliminarea fizică a inamicului de pe un teritoriu pentru a-l ocupa. Câmpul de luptă a rămas liniar, deși, prin comparație cu războaiele de primă generație, lățimea zonei de confruntare a crescut proporțional cu raza de acțiune a armamentului, în principal a artileriei și, mai târziu, a aviației. Încercarea de a sparge zonele fortificate a condus la clasicele blocaje poziționale înregistrate în Primul Război Mondial, caracterizate de pierderi de vieți omenești și risipă de resurse la un nivel fără precedent. Strategia din spatele războaielor de generația a doua se baza pe mobilizarea de armate și resurse la un nivel superior față de cel al inamicului. Comunicațiile și logistica au beneficiat de noi soluții tehnologice, precum telegraful și căile ferate. Tactica necesita un stres mai mic decât în prima generație și putea fi rezumată de maxima franceză „artileria cucerește, infanteria ocupă”⁵.

Războiul de generația a treia (războiul manevrier)

Acest tip de război este caracterizat de acțiuni manevriere ample, executate în viteză, care pun în valoare superioritatea tehnologică proprie. Războiul de generația a treia a constituit un răspuns la creșterea puterii de foc pe câmpul de luptă. Realizând faptul că nu se poate compara material cu un adversar superior, din cauza unei baze industriale mult mai slabe, Germania a transformat modul de ducere a luptei punând accent pe acțiuni manevriere în detrimentul celor de uzură, tacticile de generația a treia fiind cu adevărat non-liniare și surprinzătoare pentru adversar. Atacul s-a bazat pe pătrundere pentru încercuirea forțelor principale ale inamicului și, ulterior, nimicirea acestora, mai degrabă decât pe confruntarea directă. Dispozitivul de apărare a avut cel puțin adâncime operativă, ceea ce a facilitat permiterea pătrunderii inamicului, care, ulterior, era nimicit prin contraatacuri executate de eşaloanele din spate (apărare mobilă). Chiar dacă o parte a tacticilor utilizate în războiul de generația a treia apăruseră deja la sfârșitul Primului Război Mondial, acestea au fost

dezvoltate de apariția binomului tanc-avion, fapt care a adus o schimbare majoră la nivel operativ, materializată în conceptul de „blitzkrieg”.

Războiul de generația a patra (războiul asimetric)

Războaiele care au urmat celui de-al Doilea Război Mondial (Coreea, Vietnam, Afganistan, Cecenia, Irak și, din nou, Afganistan) au păstrat unele caracteristici ale războiului de generația a treia (în special abordarea manevrieră și concentrarea efortului operațional pe anumite faze și momente, precum și utilizarea unor acțiuni de nivel tactic sau operativ pentru atingerea unor obiective de nivel strategic), dar s-au adaptat noului inamic și modului de operare a acestuia. Astfel, au fost dezvoltate noi forme de răspuns la acțiunile adversarilor, materializate, în principal, în acțiuni de insurgență, gherilă, terorism etc. Majoritatea confruntărilor care au urmat celui de-al Doilea Război Mondial au fost duse de către o putere militară majoră împotriva unui inamic mult mai slab dezvoltat sau depășit tehnologic, chiar dacă era susținut, de cele mai multe ori, de un alt stat puternic dezvoltat. Caracteristicile războiului de generația a patra au devenit evidente după încheierea de facto a Războiului Rece, odată cu trecerea la un sistem internațional unipolar, și au fost cel mai bine reprezentate de „războiul total împotriva terorismului”, declanșat de SUA după atacurile teroriste din septembrie 2001.

Războiul de generația a patra este în esență un război neconvențional, asimetric, în antiteza conceptului tradițional de război definit de primele trei generații. Distincția dintre război și pace este estompată, iar acțiunea militară are un caracter neliniar până la punctul în care nu există un spațiu de confruntare bine definit. Dispare, de asemenea, distincția dintre civili și militari, fenomenul absorbind toate segmentele societății. Este un război în care culturile pot fi în conflict și în care, alături de forțele militare, sunt implicați o serie de factori politici, sociali și economici. Războiul asimetric poate fi declanșat, în egală măsură, atât de către state, cât și de actori non-statali, transnaționali sau subnaționali.

Progresul în domeniul comunicațiilor permite inamicului să realizeze o largă dispersie și să acționeze în formațiuni mici, dispuse în rețea, cu o dependență minimă de logistica centralizată, fără a oferi ținte în masă și cu o mare capacitate de manevră.

Au loc angajamente tactice scurte și de mică intensitate și, deși războiul este unul de durată, nu există lupte. Neliniaritatea este atât de extremă încât confruntarea se realizează la nivelul întregii societăți a inamicului. Devin determinante sprijinul populației pentru război și cultura inamicului. Sponsorii statali ai inamicului nu-l pot susține în mod deschis, ceea ce face preferabilă adoptarea unui caracter non-statal.

În războaiele din primele trei generații victoria era obținută odată cu înfrângerea armatei oponentului; în acest tip de război, victoria este obținută atunci când este afectată voința actorului statal de a continua lupta. Acțiunile militare nu mai au ca obiectiv distrugerea capabilităților militare, ci inducerea unui impact psihologic major atât la nivelul societății în care are loc confruntarea, cât și la nivelul societății statului beligerant. Această realitate schimbă rolul pe care mass-media îl joacă pe parcursul conflictului până la punctul în care acestea sunt utilizate pentru a submina susținerea populației din statul beligerant pentru continuarea conflictului armat. Prin urmare, managementul comunicării publice are efecte tactice, acest tip de conflict fiind bazat pe informații mai mult decât toate celelalte generații de război.

Războiul asimetric a produs un efect major asupra modului în care sunt organizate, echipate și instruite forțele militare tradiționale. Aceste schimbări nu au presupus neapărat desființarea capabilităților asociate războiului de manevră (blindate, infanterie, artilerie, aviație, marină etc.), ci mai degrabă modificări ale modului în care acestea sunt utilizate. În acest context, sporește importanța capacităților de intelligence și a forțelor speciale, înțelegerea mediului de confruntare și viteza de acțiune constituind atuuri pentru a asigura o acțiune ofensivă sau defensivă rapidă și precisă. Sporește, de asemenea, importanța armelor de precizie înaltă pentru limitarea maximă a victimelor colaterale.

Către războiul de generația a cincea

Relansarea competiției globale dintre marile puteri și realitățile generate de războiul de generația a patra creează premisele unei noi schimbări de paradigmă. În acest context, asistăm la „apariția războiului hibrid, o combinație de război convențional, neregulat, economic, energetic, cibernetic, război identitar și prin *proxy*, combinate într-o formă complicată și instabilă, cu un război limitat, dar în același timp și fără limite, fără restricții, în sensul utilizării capabilităților de toate tipurile, fără reguli: capabilități infracționale, economice și informaționale, propaganda și războiul neregulat prin intermediari, insurecție și terorism, toate în același teatru, unde, potrivit abordării realiste a lui Machiavelli, *tous les coups sont bons!*”⁶.

După cel de-al Doilea Război Mondial riscul utilizării armamentului nuclear a făcut ca o confruntare militară directă de anvergură între marile puteri să devină improbabilă. Ca urmare, conflictele armate dintre state s-au manifestat mai mult sub forma războaielor locale, izolate, purtate prin intermediari de către puterile globale, în încercarea de a evita o confruntare de amploare. Când s-au implicat, statele și-au mascat acțiunile, utilizând entități non-statale (entități etnice manipulate, grupări teroriste, rețele de criminalitate organizată sau companii de securitate). Cel mai elocvent exemplu de conflict hibrid este cel desfășurat în 2014 de Rusia împotriva Ucrainei, care a condus la reconfigurarea granițelor Ucrainei prin anexarea de către Rusia a Peninsulei Crimeea, precum și la blocarea aspirațiilor euro-atlantice ale Kievului prin crearea conflictului înghețat din Donbas.

Disponibilitatea unor puteri globale, precum Rusia sau China, de a contesta echilibrul de putere stabilit după finalizarea Războiului Rece determină o serie de schimbări importante în dinamica confruntărilor intra și interstatale.

O serie de evoluții tehnologice pun sub semnul întrebării *statu-quo*-ul. Spre exemplu, dezvoltarea sistemelor de apărare anti-rachetă, în special a celor destinate contracarării rachetelor balistice intercontinentale, induce ideea posibilității managementului consecințelor unui

război nuclear. Același efect îl au dezvoltarea armamentului nuclear sub-strategic și relaxarea prevederilor doctrinelor nucleare din unele state, în sensul luării în considerare a opțiunii de inițiere a unui atac nuclear în alte circumstanțe decât cele ale răspunsului la un atac similar, existența unui număr important de state nucleare în afara cadrului juridic delimitat de Tratatul de Neproliferare Nucleară, existența unor state care aspiră la statutul de putere nucleară, proliferarea rachetelor balistice etc.

Parametrii confruntării interstatale sunt, de asemenea, complicați prin recunoașterea importanței altor domenii de confruntare pe lângă domeniile non-militare deja recunoscute (război informațional, ideologic, economic, cultural-religios). Astfel, un număr de state, între care SUA, Rusia, China sau Franța, întreprind măsuri de reorganizare militară în sensul includerii și dezvoltării de capabilități destinate derulării de acțiuni militare în mediile cibernetic și spațial.

Războiul de generația a cincea va primi, fără îndoială, o definiție unanim acceptată în viitorul apropiat, odată ce noi tehnici, tactici și proceduri vor fi dezvoltate și testate. Până atunci este de așteptat ca direcția de evoluție a confruntării să includă atât elemente ale războiului manevrier, cât și pe cele ale războiului asimetric, suprapuse și extinse pe tot mai multe domenii de confruntare. Modul de abordare a confruntării militare și nu numai, cunoscut în prezent sub denumirea de război hibrid, poate constitui un model cu privire la direcția de dezvoltare a fenomenului, dar este de așteptat să îl depășească în anvergură și complexitate.

În linii mari, este probabil ca generația a cincea a confruntării să fie, în egală măsură, culturală, socială și economică, ceea ce va face dificilă distincția dintre pace și război, statul/statele agresate nerealizând că se află, de fapt, în război. În unele situații, „acțiunile nu vor fi în mod obligatoriu îndreptate împotriva statului, ci, mai degrabă, vor avea ca scop erodarea autorității instituțiilor statului respectiv”⁷. Acest lucru poate fi văzut ca un război conceput să schimbe regimul democratic al unui stat, ordinea constituțională a acestuia și chiar să aibă ca rezultat afectarea integrității teritoriale.

Dacă într-un război convențional influențarea procesului de decizie politică al adversarului se face prin aplicarea de strategii menite să neutralizeze forța militară a statului în timp ce se urmărește izolarea populației, într-un război de tip hibrid sunt aplicate strategii de influențare a opiniei publice și de izolare a factorului militar pentru obținerea aceluiași efect.

În ceea ce privește fizionomia conflictului de generația a cincea, până în prezent nu se înregistrează o viziune unitară la nivel internațional. Potrivit directorului general al Centrului pentru Securitate și Cercetări Strategice al Academiei Naționale de Apărare din Letonia, Jānis Bērziņš⁸, Armata rusă a dezvoltat o strategie pe care a denumit-o „Război de nouă generație”, potrivit căreia noul tip de conflict va combina tactici asimetrice, neliniare și neconvenționale cu forme moderne ale războiului tradițional, în următorii pași:

- *Prima fază*: război asimetric non-militar, care cuprinde agresiune informațională, culegere de informații, măsuri psihologice, ideologice, diplomatice și economice;
- *A doua fază*: operații informaționale direcționate pentru inducerea în eroare a liderilor politici și militari, prin măsuri coordonate efectuate prin canale diplomatice, mass-media și agenții militare care implică scurgeri de date false, ordine, directive și instrucțiuni;
- *A treia fază*: acțiuni de intimidare, șantaj și mituire a oficialilor guvernamentali și militari cu scopul de a-i face să renunțe la atribuțiile de serviciu;
- *A patra fază*: propagandă destabilizatoare pentru a crește nemulțumirea în rândul populației, stimulată de acțiunea unor grupuri de militanți (grupuri/grupări/organizații bazate pe o identitate socioculturală comună – n.n.), escaladarea subversiunii;
- *A cincea fază*: identificarea zonelor din țară care urmează să fie atacate, impunerea de blocaje, utilizarea pe scară largă a companiilor militare private în strânsă cooperare cu unitățile armate de opoziție;

- *A șasea fază*: începerea acțiunilor militare, precedate de misiuni de recunoaștere la scară largă și misiuni subversive de toate tipurile, angajarea forțelor pentru operații speciale;
- *A șaptea fază*: operații de informații direcționate, război electronic și aerospațiale, conjugate cu hărțuirea continuă executată de forțele aeriene, concomitent cu utilizarea armelor de înaltă precizie lansate de pe diverse platforme; de asemenea, vor fi utilizate sistemele de armament cu rază lungă de acțiune bazate pe noi principii fizice de funcționare, catastrofe radiologice și ecologice, precum și arme biologice neletale;
- *A opta fază*: distrugerea punctelor de rezistență rămase prin utilizarea forțelor pentru operații speciale.

Se poate observa că, spre deosebire de alți cercetători, școala de gândire rusă continuă să ia în calcul utilizarea semnificativă a instrumentului militar și în conflictele viitoare. Această abordare este în concordanță cu documentele programatice ruse (Strategia de securitate națională, Doctrina militară, Bazele descurajării strategice etc.), justificând investițiile pe care Moscova le face în dezvoltarea noilor sisteme de armament strategic.

Un studiu canadian indică următoarele elemente drept importante pentru descrierea războiului de generația a cincea⁹:

- principalele părți implicate vor fi entități cu o identitate socio-culturală comună (incluzând grupări de crimă organizată), ceea ce face ca acest tip de conflict să fie centrat pe populație și nu pe instituțiile statale;
- este foarte probabil ca naționalismul, care să nu fie neapărat relaționat și identității statale, să constituie o platformă de promovare a conflictului;
- aceste entități vor putea prelua din atribuțiile statului, atunci când acesta devine incapabil să asigure securitatea, fiind girate la rândul lor de populația din teritoriul pe care îl controlează;
- la vedere conflictul de generația a cincea va fi dus de grupuri împotriva unui stat și nu de state împotriva statelor.

Alți cercetători¹⁰ prevăd conflictul de generația a cincea ca fiind asumat atât de actori statali, cât și de actori non-statali, pe linii de efort care includ domeniile informaționale și *cyber*, printr-un mix de acțiuni cinetice și non-cinetice. Actorii statali implicați vor evita confruntarea armată, iar rezultatele vizate vor include obiective de nivel tactic – prin acțiuni de *hacking*, obiective de nivel operativ – prin executarea de acțiuni teroriste sau relaționate acestora și obiective strategice – prin schimbarea regimului politic/ordinii constituționale din statul țintă.

Concluzii

Înțelegerea evoluției practicii războiului este importantă datorită efectelor pe care această interpretare o are asupra modului în care este organizată și instruită forța militară a unui stat. Formarea unei armate performante constituie un demers care implică resurse financiare semnificative și presupune cicluri temporale prelungite. O ipoteză de planificare eronată va avea ca efect eșecul acțiunii militare pe câmpul de luptă și incapacitatea statului de a contracara eficient amenințările la care este supus. Factorul politic are, de asemenea, datoria de a înțelege contextul în care poate aplica soluții militare la probleme de securitate și limitările pe care această variantă de acțiune le presupune. Probabil, modul de reacție într-un mediu de securitate caracterizat de confruntări de generația a cincea va impune angajarea de pachete acționale care să includă combinații de mijloace militare, informaționale, economice, culturale și de orice altă natură, coordonate în mod unitar și coerent.

Războiul hibrid reprezintă, în fapt, o avanpremieră a ceea ce va însemna războiul de generația a cincea. Acesta din urmă va prelua din caracteristicile tipurilor anterioare de război, în particular atributele manevriere și asimetrice, extinse pe domenii multiple, efectele confruntării pe un domeniu fiind resimțite dincolo de limitele acestuia. Factorul militar își va menține importanța în economia de forțe și mijloace angajate într-o confruntare, dar nu mai poate fi izolat de ceilalți factori.

Deși confruntările militare vor include din ce în ce mai mult entități non-statale, războiul de

generația a cincea va rămâne, în esență, reflecția relansării competiției globale dintre state. Este de așteptat ca acesta să se manifeste de-a lungul liniilor de demarcație a zonelor de influență a statelor și alianțelor dintre state, contribuind la delimitarea acestora. Foarte probabil, în pofida confruntării, actorii statali vor fi interesați să mențină iluzia stării de pace pentru a face dificilă, din punct de vedere legal, acțiunea forțelor armate. Modelarea strategică va fi executată de statul agresor, în primul rând la adresa sistemului politic și social din statul țintă pentru a crea nemulțumire în rândul populației și, ulterior, la nivel internațional pentru a obține legitimitate.

Nu în ultimul rând, este de așteptat ca transformarea naturii confruntării și a câmpului de luptă să impună revizuirea standardelor etice aplicate pe timpul acțiunilor militare, cele utilizate în prezent fiind dezvoltate pentru a răspunde realităților războaielor din primele generații.

Bibliografie:

1. CHIFU Iulian, „Război hibrid, „lawfare“, război informațional. Războaiele viitorului“, https://adevarul.ro/international/in-lume/razboi-hibrid-lawfare-razboi-informational-razboaiele-viitorului-1_56f281ab5ab6550cb8246783/index.html.
2. SUCIU F.B., „Războiul zilelor noastre. Tablouri cu scene de luptă“, <https://intelligence.sri.ro/razboiul-zilelor-noastre-tablouri-cu-scene-de-lupta/>.
3. CASIS-Vancouver, *Contemporary conflict & the fifth generation of warfare*, The Journal of Intelligence, Conflict and Warfare, https://www.researchgate.net/publication/326194488_Contemporary_Conflict_The_Fifth_Generation_of_Warfare, accesat la data de 11.08.2020.
4. KATOCH Ghanshyam Singh, *Fourth Generation War: Paradigm For Change*, Iunie 2005, disponibil la <https://apps.dtic.mil/sti/pdfs/ADA435502.pdf>
5. Lt. col. NISAR Maaz, *5 GW and hybrid warfare. Its implications and response options*, p.20. <https://bdex.eb.mil.br/jspui/bitstream/123456789/2827/1/MO%200023%20-%20MAAZ.pdf>
6. <https://content.sciendo.com/view/journals/jobs/5/1/article-p17.xml>, accesat la data de 11.08.2020.

- ¹ Cf. F.B. Suciu, „Războiul zilelor noastre. Tablouri cu scene de luptă“, <https://intelligence.sri.ro/razboiul-zilelor-noastre-tablouri-cu-scene-de-lupta/>.
- ² Ibidem.
- ³ Ghanshyam Singh Katoch, *Fourth Generation War: Paradigm for Change*, iunie 2005, disponibil la <https://apps.dtic.mil/sti/pdfs/ADA435502.pdf>
- ⁴ Idem 3
- ⁵ Idem 4
- ⁶ Cf. Iulian Chifu, Război hibrid, „lawfare“, război informațional. Războaiele viitorului, https://adevarul.ro/international/in-lume/razboi-hibrid-lawfare-razboi-informatiional-razboaiele-viitorului-1_56f281ab5ab6550cb8246783/index.html.
- ⁷ CASIS-Vancouver, Contemporary conflict & the fifth generation of warfare, *The Journal of Intelligence, Conflict and Warfare*, vol. 1, no. 1, 2018, https://www.researchgate.net/publication/326194488_Contemporary_Conflict_The_Fifth_Generation_of_Warfare, accesat la data de 11.08.2020.
- ⁸ După <https://content.sciendo.com/view/journals/jobs/5/1/article-p17.xml>, accesat la data de 11.08.2020.
- ⁹ După CASIS-Vancouver, “Contemporary conflict & the fifth generation of warfare“, *The Journal of Intelligence, Conflict and Warfare*, vol. 1, no. 1, 2018, https://www.researchgate.net/publication/326194488_Contemporary_Conflict_The_Fifth_Generation_of_Warfare, accesat la data de 11.08.2020.
- ¹⁰ După lt. col. Maaz NISAR, “5 GW and hybrid warfare. Its implications and response options“, p.20. <https://bdex.eb.mil.br/jspui/bitstream/123456789/2827/1/MO%200023%20-%20MAAZ.pdf>, accesat la data de 11.08.2020.

FORȚELE AERIENE, FACTOR DE DESCURAJARE ÎN PROCESUL DE ESCALADARE A CRIZELOR

Vasile-Cristian ONESIMIUC*

Abstract

Crisis situations tend to become more and more frequent in today's security environment. Knowing the situation on the basis of accurate information, available at the right time, can determine decision-makers to use the air force as a credible deterrent measure to stop the escalation of the ongoing crisis. This decision should be taken on the basis of a realistic analysis process, which would lead to a de-escalation of the situation and without unrealistic expectations. Quality of the air assets, implications of air force use, its limitations, associated risks and expected benefits must be seen as a unitary system by decision-makers in the situation assessment and decision-making process. However, the use of the air force as a deterrent measure, similar to other deterrents, does not guarantee the elimination of the risk of crisis escalation.

Keywords: Air Forces, intelligence, deterrence, decision, crisis, risk.

Evoluția mediului global de securitate, instabilitatea, dinamica amenințărilor, riscurilor și vulnerabilităților sunt marcate de apariția, la un moment dat, a unor situații de criză, care determină un răspuns din partea factorilor de decizie, ca modalitate de adaptare la noile realități ale mediului de securitate. Modul în care se realizează această adaptare, precum și măsurile adoptate pentru depășirea situației de criză apărute, modelează relațiile de putere între actorii implicați, dar în același timp determină o modificare a mediului de securitate și creează premisele apariției unei noi situații de criză în viitor.

Manualul de planificare a operațiilor definește „criza”/„situația de criză” ca fiind „acea stare în care se poate afla un sistem/sistem de sisteme - un grup organizat, o parte a unei națiuni, o națiune, un grup de națiuni, actori statali/non-statali etc. - delimitată în timp și spațiu, alta decât starea de pace. În sistemul nostru de drept există o definiție legală pentru următoarele stări, altele decât starea

de pace: starea de urgență, starea de asediu, starea de mobilizare, starea de război”¹.

La nivel internațional nu există definiții unanim acceptate ale termenului de criză. Dicționarul explicativ al limbii române definește „criza” drept „manifestare violentă a contradicțiilor (economice, politice, ideologice, militare), moment critic, periculos, decisiv”², iar termenul „escaladare” este definit ca fiind „extindere treptată a unei acțiuni, a unui conflict”³.

Curba de dezvoltare a crizelor⁴ are marcate pe cele două axe, de intensitate și durată, praguri de trecere pentru fiecare dintre etapele de dezvoltare a crizelor. Având în vedere cele două definiții, momentul de criză 4 poate escalada în intensitate și să se extindă, trecând în etapa de dezvoltare 5, de conflict violent, sau poate descrește în intensitate, evoluând spre detensionare, fără a fi nevoie să treacă prin etapa de conflict violent. În lumea reală, cel mai adesea desfășurarea crizelor este destul de rapidă, iar unele din etapele prezente în fig.1 nu sunt foarte clar delimitate, ele putând fi

*Expert în cadrul Ministerului Apărării Naționale.

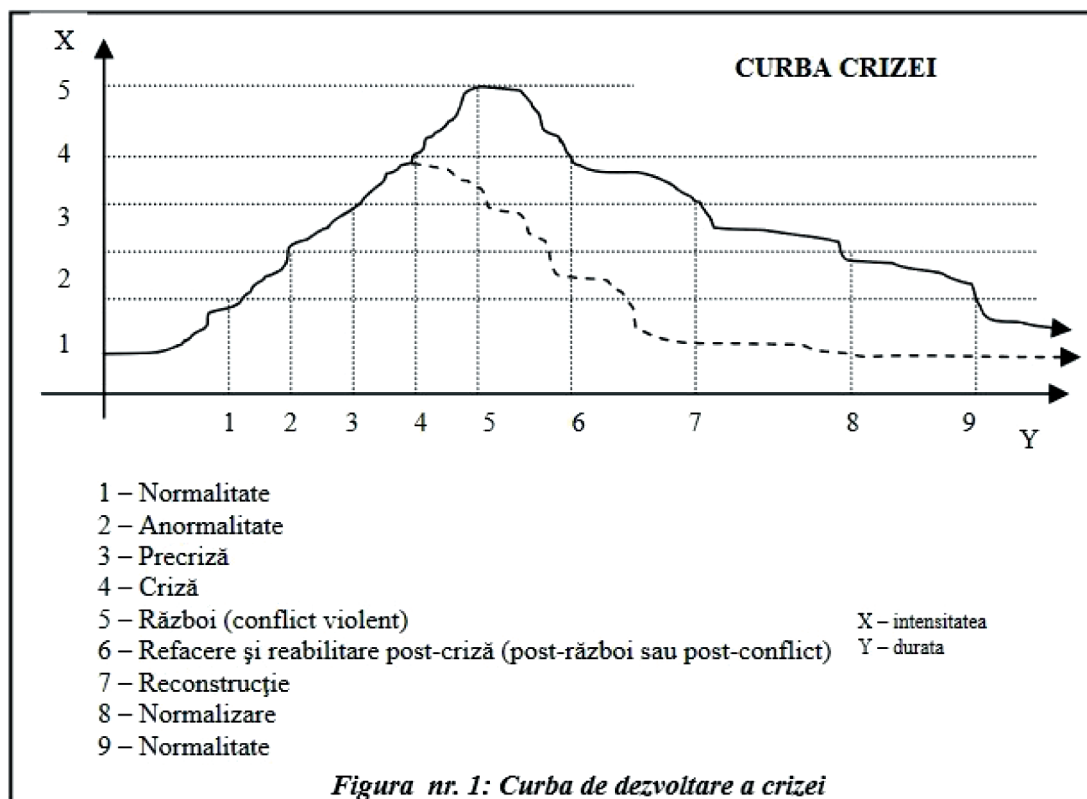


Figura nr. 1: Curba de dezvoltare a crizei

întrepătrunse pe anumite segmente de dezvoltare a crizei.

Din punct de vedere al actorilor implicați și al localizării crizei putem avea crize la nivel local, național, regional sau internațional. Nivelul de dezvoltare al crizei necesită o analiză și un răspuns adecvat din partea factorilor de decizie, pe fiecare nivel, gestionarea crizelor fiind un proces complex care solicită din plin resursele autorităților. Etapele de gestionare a crizei⁵ sunt următoarele: prevenirea, identificarea, schimbul de informații, coordonarea, luarea deciziilor, iar ciclul de gestionare a crizei trebuie reluat continuu pentru a reuși integrarea noilor informații pe măsură ce acestea devin disponibile. Nesoluționarea unei crizei încă din fazele incipiente poate conduce la escaladarea acesteia în conflict; mai mult decât atât, gestionarea crizei trebuie să fie în măsură să prevină agravarea situației și a controverselor care au generat situația inițială, pe considerentul creării premiselor de revenire la starea de normalitate după detensionarea situației de criză.

Crizele militare au o multitudine de indici⁶ care pot dezvălui evoluțiile ulterioare, cum ar fi: „concentrarea de forțe în proximitatea frontierelor naționale, cu notificarea sau nu

a activităților; realizarea de alianțe militare cu scop nedeclarat sau mascat; reorganizări ale sistemului militar din unele state vecine; redислоări de comandamente ale marilor unități și unități în apropierea frontierelor; pregătiri intense ale marilor unități de aviație; concentrări în baze militare, exerciții, simulări; antrenamente într-o concepție de învățământ sau alte forme de mascare; reorientări doctrinare ca urmare a mutațiilor produse în politica militară a unora din statele vecine; nerespectarea culoarelor de zbor internaționale de către aeronavele militare și civile; dotarea masivă a forțelor armate ale unor state vecine cu tehnică militară performantă și armament modern; folosirea pe timpul aplicațiilor statelor majore a scenariilor tactice ce vizează părți din teritoriul național; penetrarea rețelelor de comunicații militare în scopul procurării de informații și date despre starea unităților militare dintr-o anumită zonă; intensificarea acțiunilor de sustragere de armament, muniție, echipament și tehnică militară din depozitele armatei; sustrageri repetate de materiale explozive de la exploatarea miniere și geologice; apariția și proliferarea grupurilor organizate ilegal care desfășoară acțiuni de tip terorist”. Multitudinea de indici

care pot avertiza cu privire la iminența unei crize, prin numărul ridicat al acestora, pot îngreuna procesul de evaluare a situației.

Cunoașterea acestor indici, coroborată cu informațiile disponibile factorilor de decizie, trebuie să asigure statului capacitatea de adaptare, anticipare și răspuns adecvat la aceste provocări de securitate. În prezent, riscul de declanșare a unui conflict armat major între principalele puteri se menține redus⁷, conform Strategiei Naționale de Apărare a Țării 2020-2024. De asemenea, riscul declanșării unui conflict armat interstatal este considerat ca fiind redus, dar sunt identificate riscuri generate de volatilitatea stării de securitate din Balcanii de Vest, alături de focarele de conflict din Regiunea Extinsă a Mării Negre.

Armata României, prin misiunile pe care le execută, poate participa la operații de răspuns la crize, în vederea promovării stabilității regionale și globale. Unul dintre obiectivele militare naționale este reprezentat de limitarea duratei și influenței unei acțiuni militare ostile de natură să genereze o criză sau situație de instabilitate, iar pentru aceasta trebuie asigurată atât capacitatea statului de a anticipa posibile situații care pot escalada în crize, precum și modalități eficiente de răspuns la acestea.

În cadrul acestor misiuni, așa cum este stipulat în cadrul Strategiei Militare a României⁸, Forțele Aeriene române, pe lângă misiunile de apărare a spațiului aerian și a spațiului comun al Alianței, participă, printre altele, la rezolvarea situațiilor de urgență și îndeplinirea angajamentelor internaționale. Capabilitățile forțelor aeriene, pregătite de luptă permanent, în condițiile în care se pot disloca rapid forțele și mijloacele din dotare, asigură o capacitate ridicată de răspuns la crize, utilizarea acestora putând fi una dintre opțiunile de răspuns aflate la dispoziția autorităților statului. Misiunile pe care le pot îndeplini forțele aeriene sunt variate, dar nu trebuie pierdut din vedere faptul că fiecare misiune are particularitățile ei și, ca urmare, de fiecare dată este necesară adaptarea răspunsului forțelor aeriene la situația particulară întâlnită. Forțele aeriene sunt o componentă importantă pentru asigurarea succesului unei operații militare, răspunsul la crize putând fi

executat ca o operație de sine stătătoare sau ca parte a unei operații majore pe o durată extinsă de timp, care să includă acțiuni de luptă⁹. Din punct de vedere al acțiunilor care pot fi desfășurate, se pot aminti aplicarea zonelor de excludere aeriană, asigurarea libertății de acțiune în spațiul aerian, evacuarea non-combatanților, acțiuni de lovire, misiuni de sprijin sau asistență umanitară.

John Kriendler¹⁰ a analizat conflictele din Balcani și a identificat importanța asigurării avertizării timpurii în cadrul managementul crizelor. Avertizarea timpurie în cazul crizelor iminente este vitală, acțiunile executate timpuriu în mod corect putând conduce la evitarea unor consecințe negative grave. Cu toate că informațiile pot fi disponibile pentru realizarea avertizării timpurii, pe baza indicilor privind dezvoltarea crizei, este dificil de determinat cum și când este cel mai bine de intervenit în cadrul unei crize pentru a restabili starea de normalitate. Este de la sine înțeles că implicarea forțelor se va realiza pe baza unei analize obținute cât mai rapid, dar în mod corect, pentru adoptarea unui curs de acțiune optim pentru obținerea rezultatelor vizate.

Avertizarea timpurie poate oferi mai mult timp pentru analiză, pregătire și planificare a planurilor de răspuns pentru participarea la criză. Având la dispoziție informații încă din fazele incipiente, se pot stabili obiective realiste, cursuri de acțiune de rezervă, analiza reacției de răspuns din partea actorilor implicați în criză, precum și eventuale cursuri de dezvoltare ulterioară a crizei. John Kriendler a subliniat importanța înțelegerii avertizării timpurii ca un proces ciclic prin care o potențială criză, risc sau amenințare este evaluată, problemele sunt definite, iar pe baza acestora sunt elaborate liste de indicatori critici. Este evident că eficiența avertizării timpurii este dependentă de modalitatea ulterioară de integrare în gestionarea crizei și în modalitățile de răspuns aflate la dispoziția autorităților.

Alegerea celei mai bune modalități de răspuns este un proces complicat, în dinamică, aflat în continuă actualizare a informațiilor cu privire la desfășurarea crizei. Desemnarea forțelor aeriene ca modalitate de răspuns la criză, în vederea prevenirii escaladării acesteia,

conduce la întrebarea firească dacă forțele aeriene sunt suficiente pentru gestionarea riscului de escaladare a crizei.

După cum se poate ușor observa, decizia de utilizare a forțelor aeriene ca factor de descurajare nu este o hotărâre ușor de luat; mai mult decât atât, implicarea acestora nu soluționează în mod automat criza și, cel mai probabil, trebuie luate și alte măsuri pentru gestionarea situației. Dacă în urma analizei se ajunge la concluzia că forțele aeriene sunt modalitatea de răspuns potrivită, se pune întrebarea dacă ar trebui stabilite anumite linii sau praguri în procesul de escaladare al crizelor care să conducă la escaladarea modalităților de răspuns¹¹ pe măsură din partea forțelor aeriene. Cum vor fi stabilite aceste praguri din punct de vedere al forțelor aeriene pentru gestionarea crizei, cât de important este ca acestea să fie cunoscute și comunicate părților implicate în conflict, astfel încât să nu existe elemente de incertitudine care să poată conduce la escaladarea neintenționată a crizei? Indiferent de decizia finală, este important de subliniat faptul că pentru detensionarea crizei sunt necesare măsuri sincronizate din punct de vedere politic și militar; utilizarea forțelor aeriene ca factor de descurajare trebuie făcută în mod controlat, iar dozarea acțiunilor militare trebuie astfel realizată astfel încât în fiecare moment să mai fie posibil dialogul și soluționarea pașnică a crizei. Nimeni nu poate garanta, pe baza unor informații cel mai adesea incomplete, care este cel mai bun curs de acțiune de urmat, decizia de utilizare a forțelor aeriene putând să sugereze o dorință de implicare redusă în evoluția evenimentelor, însă capacitatea de reacție rapidă și posibilitățile de acțiune ale forțelor aeriene vor determina o modificare a comportamentului actorilor implicați în situația de criză.

Limitările utilizării forțelor aeriene în cadrul crizelor

Decizia de utilizare a forțelor aeriene, ca modalitate de răspuns și descurajare a escaladării crizelor, trebuie să fie rezultatul unei analize foarte pragmatice, care să ia în considerare limitările¹² evidente care afectează acțiunile mijloacelor aeriene.

Una dintre cele mai evidente constrângeri este reprezentată de durata limitată în care mijloacele aeriene pot să execute misiunile de zbor. Mijloacele aeriene ofensive pot să-și extindă durata de zbor prin executarea realimentărilor în aer, dar în acest caz trebuie luați în considerare alți factori, cum ar fi starea de oboseală a personalului navigant. Chiar dacă prin realimentarea în aer se obține o durată de zbor care este determinată de capacitatea echipajului de a diminua efectele oboselii și a menține starea de alertă, necesitatea reînarmării aeronavei rămâne un factor de limitare decisiv. Sistemele de armament utilizate în prezent nu permit depășirea acestei limitări, iar pe termen scurt nu se întrevăd modalități practice care să rezolve acest impediment major. Utilizarea mijloacelor aeriene fără echipaj la bord poate să elimine limitarea în ceea ce privește extinderea duratei de zbor, prin eficientizarea sistemelor de propulsie, dar rămâne nerezolvată deficiența majoră prezentă și în cazul aeronavelor cu echipaj la bord, cea a imposibilității reînarmării în aer.

O limitare nu atât de evidentă, dar cel puțin la fel de importantă din perspectiva descurajării escaladării crizei, o reprezintă dependența forțelor aeriene de informații precise, care să fie disponibile la momentul oportun, cu un grad ridicat de încredere. Evaluarea riscului pe baza informațiilor disponibile trebuie să asigure factorilor de decizie la nivel strategic fundamentul pentru elaborarea deciziei de implicare a forțelor aeriene în situația de criză, momentul oportun, nivelul forțelor alocate și modalitățile practice de realizare a celor decise la nivel politic.

Forțele aeriene au nevoie de un flux de informații continuu, începând încă din etapele premergătoare implicării acestora în misiuni de zbor. Informațiile trebuie să fie în măsură să asigure protecția aeronavelor și facilităților proprii, dar în același timp să permită cunoașterea amenințărilor la adresa forțelor proprii, atât la sol, cât și în aer. Cunoașterea asigură reducerea incertitudinilor, scade riscul fratricidului și permite continuarea operațiilor aeriene. Dependența de informații este cu atât mai vizibilă în cadrul procesului de targeting, lipsa de informații precise putând determina executarea unor misiuni care să

producă victime colaterale, iar acest lucru este cu siguranță unul dintre evenimentele care nu sunt dorite.

Intervenția forțelor aeriene în cadrul unei crize necesită o apropiere a bazelor aeriene de zona de conflict, astfel încât aeronavele să poată executa misiunile de zbor. Această apropiere de zonele de conflict crește nivelul riscurilor la adresa facilităților aeroportuare și a aeronavelor utilizate. Pentru reducerea riscurilor pe timpul executării misiunilor de zbor sunt necesare misiuni de recunoaștere, atât pentru cunoașterea situației din teren, cât și pentru prevederea acțiunilor actorilor implicați în situația de criză. Ciclul de luare a deciziilor de la nivelul forțelor aeriene, bazat pe informații precise, disponibile continuu, va permite luarea unor decizii oportune pentru descurajarea dezvoltării crizei. Executarea de misiuni de patrulare aeriană cu aeronave de luptă înarmate oferă posibilitatea executării de misiuni de lovire¹³ dacă acest lucru este necesar sau dacă se decide schimbarea misiunii în aer, fapt care este cunoscut și de către actorii implicați în criză.

Importanța forțelor aeriene în cadrul sistemului de apărare este una dintre cauzele care au determinat adversarii sau potențialii adversari să aloce resurse pentru desfășurarea unor acțiuni cibernetice deliberate, cu potențial distructiv la adresa forțelor aeriene. Acest lucru a devenit din ce în ce mai vizibil în zilele noastre, domeniul cibernetic având un impact ridicat asupra desfășurării activităților forțelor aeriene. Cu atât mai mult, după luarea deciziei de implicare a forțelor aeriene în cadrul unei situații de criză, este de așteptat ca activitățile cibernetice ostile

la adresa acestora să se intensifice, aceasta putând fi una din modalitățile de răspuns a unora dintre actorii implicați la ingerința externă.

Operația Allied Force 1999

Operația aeriană a NATO¹⁵ din Kosovo, în anul 1999, a fost desfășurată pentru stoparea crizei umanitare aflate în desfășurare. Decizia de a utiliza forțele aeriene nu a fost rapidă, fiind nevoie de aproximativ un an pentru luarea acestei hotărâri, ca urmare a eșecului eforturilor diplomatice. Obiectivele campaniei aeriene urmăreau stoparea acțiunilor militare și a violențelor, pe durata celor 78 de zile fiind executate aproximativ 38.000 de ieșiri/avion și 10.484 misiuni de lovire a unor obiective, fără a fi înregistrate victime din rândul forțelor NATO. Este interesant de menționat că aeronavele AWACS au executat 10.667 de misiuni de zbor în sprijinul operațiilor desfășurate în Balcani¹⁶ între 1992 și 2004. Campania aeriană din 1999 a debutat cu misiuni de bombardament executate asupra infrastructurii de apărare aeriană, ulterior crescând în intensitate și prin utilizarea sistemelor de lovire de precizie. Pe timpul misiunii aeriene din 1999, NATO a experimentat unele din primele incidente de natură cibernetică¹⁷, în care au fost atacate servere NATO utilizate pentru serviciile de poștă electronică. Cu toate că atacul cibernetic nu a avut un impact semnificativ asupra desfășurării campaniei aeriene de bombardament, modalitatea de răspuns din partea actorilor crizei a fost adaptată raportului de forțe nefavorabil, nivelul redus de complexitate al atacului cibernetic fiind totuși un semnal de alarmă pentru NATO. Atacul a determinat alertarea factorilor de decizie cu privire la amenințările cibernetice și necesitatea adoptării unor măsuri pentru asigurarea apărării cibernetice.

Operația aeriană Unified Protector 2011

Un alt exemplu în care forțele aeriene au fost utilizate ca factor de descurajare în procesul de escaladare a crizelor a fost cazul crizei din Libia¹⁸ din anul 2011. Misiunile de luptă executate au distrus în timp foarte scurt infrastructura libiană



Figura nr. 2 Operația Allied Force¹⁴



Figura nr. 3: Operația Unified Protector

utilizată în cadrul apărării aeriene, precum și centrele de comandă și control. Succesul misiunilor de lovire s-a datorat informațiilor colectate anterior, deși în unele etape, pentru contracararea efectelor absenței forțelor terestre în Libia, au fost utilizate elicoptere de atac. Misiunea NATO¹⁹ a durat șapte luni, fiind implicate 260 aeronave, acestea executând 26.500 de ieșiri/avion, inclusiv 9700 misiuni de lovire a unor obiective. În cadrul misiunilor de zbor au fost utilizate aeronave AWACS, acestea efectuând 247 misiuni cu durata de aproximativ 2100 de ore de zbor²⁰. Este important de menționat că în paralel cu acțiunile forțelor aeriene au fost desfășurate eforturi diplomatice pentru detensionarea crizei. Din punct de vedere al forțelor aeriene, acțiunile desfășurate au reprezentat un factor de descurajare credibil în procesul de escaladare a crizei, intervenția rapidă, decisivă, adaptată la realitățile din teren, reușind să reducă pierderile de vieți în rândul populației civile, fără a înregistra pierderi din rândul forțelor proprii.

Analizând utilizarea forțelor aeriene în cele două operații amintite se evidențiază următoarele elemente:

- Simpla deținere a unor capacități ofensive nu este suficientă, ci sunt necesare cantități suficient de numeroase de mijloace aeriene de luptă pentru a asigura credibilitatea acțiunilor – acestea trebuie augmentate de aeronave AWACS, ISR, realimentare în aer, UAV, toate acestea traducându-se, în final, prin costuri ridicate ale intervenției militare. Mai mult decât atât, toate aceste mijloace aeriene

necesită o apărare eficientă, la sol și în zbor; ca urmare, sunt necesare forțe suplimentare pentru asigurarea securității fizice mijloacelor aeriene.

- Necesitatea integrării forțelor aeriene în cadrul unor coalitii pentru executarea misiunilor de zbor, atât pentru asigurarea legitimității acțiunilor executate, cât și a repartizării costurilor asociate prin împărțirea sarcinilor de zbor între membrii coalitiei.

- Posibilitatea creșterii graduale a intensității acțiunilor desfășurate de către forțele aeriene ca răspuns la dezvoltarea crizei este un alt aspect de avut în vedere la adoptarea deciziei de întreprindere a forțelor aeriene. Evaluarea acțiunilor participanților la criză necesită un flux de informații continuu (acțiunile acestora pot fi evaluate și pot fi luate decizii în deplină cunoștință de cauză). Forțele aeriene trebuie să dispună de mijloacele aeriene necesare pentru a fi suficient de credibile atunci când își manifestă anumite intenții de a impune un anumit curs de acțiune sau când se dorește obligarea participanților la criză să se supună unor restricții.

- Dislocarea rapidă după luarea deciziei de utilizare favorizează rezolvarea crizei în stadii incipiente, dar trebuie avute în vedere costurile ridicate reclamate de utilizarea forțelor aeriene, mai ales în condițiile prelungirii duratei de executare a operațiilor aeriene.

Concluzii

Forțele aeriene s-au dovedit un factor de descurajare credibil în procesul de escaladare a crizelor, dar limitările acestora trebuie avute în vedere pe timpul analizei unei potențiale crize și, ulterior, a măsurilor de răspuns la aceasta. Utilizarea judicioasă, adaptată la realitățile din teren, va menține credibilitatea forțelor aeriene, acest fapt asigurând utilizarea viitoare a acestora ca factor de descurajare la fel de eficient și cu rezultate previzibile în viitoarele potențiale crize.

Mediul de securitate se află într-o continuă schimbare, iar forțele aeriene trebuie să fie în măsură să evolueze și să se pregătească pentru a răspunde la un întreg spectru de crize (militare, politice, sociale, etc.). Sistemul de subsisteme

din cadrul forțelor aeriene trebuie înțeles ca un întreg, iar utilizarea forțelor aeriene ca factor de descurajare nu trebuie privită doar prin prisma capabilităților ofensive deținute, acestea trebuind sprijinite și de alte acțiuni, cum ar fi cele din mediul diplomatic sau politic.

Limitările forțelor aeriene din punct de vedere al calității și cantității mijloacelor trebuie analizate în directă corelație cu situația de criză, în mod realist, pentru a nu se induce la nivelul autorităților decidente așteptări nerealiste în urma deciziei de utilizare a acestor forțe ca modalitate de răspuns la criză.

Dezvoltarea forțelor aeriene, prin introducerea de aeronave moderne în înzestrare, îmbunătățirea avertizării timpurii și specializarea pregătirii personalului, va asigura premisele pentru menținerea forțelor aeriene ca factor de descurajare a procesului de escaladare a crizelor viitoare.

Bibliografie

1. ***, Manualul de planificare a operațiilor, București, 2016.
2. ***, Dicționarul explicativ al limbii române;
3. ***, Strategia Națională de Apărare a Țării pentru perioada 2020-2024, 2020.
4. ***, Strategia Militară a României, 2016.
5. ***, Annex 3-0 - Operations and Planning, Airpower and the range of military operations, 2016.

6. ***, NATO Fact Sheet, Operation Unified Protector Final Mission Stats, 2011.
7. ***, NATO role in Kosovo, Operation Allied Force, 2006.
8. ***, Kosovo Air Campaign, 2016.
9. ***, NATO Airborne Early Warning and Control Force.
10. BĂHNĂREANU., C., *Crize potențiale ce pot afecta securitatea națională: prevenirea, limitarea și soluționarea situațiilor de criză*, Editura Universității Naționale de Apărare „Carol I” București, 2011.
11. KRIENDLER, J., *Anticipating Crises*, NATO Review, 2002.
12. STANCILĂ Lucian, Gheorghe Savu, „Crizele ca manifestări ale dezechilibrului social”, în *Tendințe în evoluția fenomenului militar la început de secol*, Editura Universității Naționale de Apărare „Carol I”, 2006, p. 271, apud. Băhnăreanu, C, op cit.
13. MORGAN, E.F., Mueller, K.P, Medeiros, E.S., Pollpeter, K.L., Cliff, R., *Dangerous Thresholds. Managing escalation in the 21st century*, RAND Corporation, 2008.
14. THEILER, O., „Noi amenințări: dimensiunea cibernetică”, *Revista NATO*, 2000.
15. VĂDUVA, G., Mureșan, M., *Criza, conflictul, războiul*, Editura Universității Naționale de Apărare „Carol I” București, 2007.
16. lafiam.wordpress.com/category/unified-protector-operation.

¹ ***, Manualul de planificare a operațiilor, București, 2016, pag.187;

² *Dicționarul explicativ al limbii române*, disponibil la <https://dexonline.ro/definitie/criza>, accesat la data de 15.08.2020;

³ *Dicționarul explicativ al limbii române*, disponibil la <https://dexonline.ro/intrare/escaladare/66397>, accesat la data de 15.08.2020;

⁴ G. Văduva, M., Mureșan, *Criza, conflictul, războiul*, Editura Universității Naționale de Apărare „Carol I” București, 2007, vol. 1, pg. 58, disponibil la <http://gheorghevaduva.ro/Altevolume/crizaconflictrazboi1.pdf>, accesat la data de 15.08.2020;

⁵ C. Băhnăreanu, *Crize potențiale ce pot afecta securitatea națională: prevenirea, limitarea și soluționarea situațiilor de criză*, Editura Universității Naționale de Apărare „Carol I” București, 2011, pg.16;

⁶ Lucian Stancilă, Gheorghe Savu, „Crizele ca manifestări ale dezechilibrului social”, în „*Tendințe în evoluția fenomenului militar la început de secol*”, Editura Universității Naționale de Apărare „Carol I”, 2006, p. 271, apud. Băhnăreanu., C, op cit;

⁷ ***, *Strategia Națională de Apărare a Țării pentru perioada 2020-2024*, paragraf91, disponibil la https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf, accesat la 15.08.2020;

⁸ ***, *Strategia Militară a României*, aprobată prin Hotărârea nr. 708 din 28 septembrie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 789 din 7 octombrie 2016;

⁹ ***, Annex 3-0 - Operations and Planning, Airpower and the range of military operations, 2016, disponibil la https://www.doctrine.af.mil/Portals/61/documents/Annex_3-0/3-0-D07-OPS-Airpower-ROMO.pdf, accesat la data de 16.08.2020;

- ¹⁰ J. Kriendler, “Anticipating Crises”, *NATO Review*, 2002, disponibil la <https://www.nato.int/docu/review/2002/issue4/english/art4.html>, accesat la data de 16.08.2020;
- ¹¹ E.F. Morgan, K.P. Mueller, E.S. Medeiros, K.L. Pollpeter, R. Cliff, *Dangerous Thresholds, managing escalation in the 21st century*, RAND Corporation, 2008, pp.163-166, disponibil la <https://apps.dtic.mil/dtic/tr/fulltext/u2/a486310.pdf>, accesat la data de 17.08.2020;
- ¹² G. Fryar, “The (air) power to coerce: the role of air power in 21st century coercive diplomacy”, The Air Power Development Centre, 2012, p.59-60, disponibil la <https://airpower.airforce.gov.au/APDC/media/PDF-Files/Fellowship%20Papers/FELL38-The-Air-Power-to-Coerce.pdf>, accesat la data de 17.08.2020;
- ¹³ G. Fryar, op.cit, p.53.
- ¹⁴ ***, *NATO role in Kosovo, Operation Allied Force*, 2006, disponibil la <https://www.nato.int/kosovo/all-frcce.htm>, accesat la data de 17.08.2020;
- ¹⁵ ***, *Kosovo Air Campaign, 2016*, disponibil la https://www.nato.int/cps/en/natohq/topics_49602.htm, accesat la data de 17.08.2020;
- ¹⁶ ***, NATO Airborne Early Warning and Control Force Balkans 1992-2004, <https://awacs.nato.int/operations/past-operations>, accesat la data de 17.08.2020;
- ¹⁷ O. Theiler, „Noi amenințări: dimensiunea cibernetică“, *Revista NATO*, 2000, disponibil la <https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/RO/index.htm>, accesat la data de 18.08.2020;
- ¹⁸ G. Fryar, op.cit, pp.73-83;
- ¹⁹ ***, NATO Fact Sheet, Operation Unified Protector Final Mission Stats, 2011, disponibil la https://www.nato.int/nato_static/assets/pdf/pdf_2011_11/20111108_111107-factsheet_up_factsfigures_en.pdf, accesat la data de 17.08.2020;
- ²⁰ ***, NATO Airborne Early Warning and Control Force 2011 Operation Unified Protector, disponibil la <https://awacs.nato.int/operations/past-operations>, accesat la data de 17.08.2020;

IMPACTUL CRIZEI MEDICALE GENERATE DE PANDEMIA DE COVID-19 ASUPRA ACTORILOR STATALI

*Alba Iulia Catrinel POPESCU**

Abstract

History lessons have shown that major epidemics have disrupted the global order that was in place at a certain moment. At present, we are facing not an epidemic, but a pandemic crisis that influences the evolution of the current international system, especially of the main actor within it – the nation-state.

From this perspective, our article tries to identify the ways in which the present COVID-19 crisis will transform the political, economic, social, ecological and military dimensions of the nation-state security. In the digital age, the impact of the current COVID-19 pandemic could herald a paradigm shift in the architecture of the international system.

Keywords: *pandemic crisis, COVID-19, world order, nation-state, international community.*

Dintotdeauna, marile epidemii au anunțat sfârșitul unei ordini mondiale și începutul alteia, noi. Așa s-a întâmplat în Antichitate, cu ciuma antonină (165-180), care a ucis 5 milioane de oameni și a grăbit sfârșitul păcii romane sau, în Evul Mediu timpuriu, cu ciuma lui Iustinian (541 – 542), care a ucis circa 10% din populația cunoscută a lumii, declanșând declinul Imperiului Bizantin. La fel s-a întâmplat și ulterior, în Evul Mediu târziu, cu epidemia de ciumă bubonică, numită și „moartea neagră” (1346-1353), care a secerat 60% din populația Europei și a creat contextul apariției Renașterii sau cu marile epidemii de ciumă, din cea de-a doua jumătate a secolului al XVII-lea, care au anunțat epoca Iluminismului și a industrializării. Și, tot așa s-a întâmplat și cu marea gripă spaniolă (1918-1920), responsabilă de mai mulți morți decât Primul Război Mondial, care a anunțat regimurile totalitare ale secolului XX, comunismul și nazismul, și a pus bazele guvernantei globale a sănătății prin înființarea, în 1920, a Organizației pentru Sănătate a Ligii Națiunilor, devenită,

ulterior, în 1948, Organizația Mondială a Sănătății (OMS). Chiar și la noi, ciuma lui Caragea, din 1813, a precedat marile evenimente care, peste 8 ani, aveau să sfârșească domniile fanariote din Țările Române și aveau să creeze premisele Revoluției de la 1848.

Astăzi, în epoca interconectării și a urbanizării, nu mai vorbim despre o epidemie, ci despre o pandemie, care a cuprins toate continentele, cu excepția Antarcticii, și a infectat, până în prezent, peste 20 milioane de oameni, ucigând peste 730.000¹. O pandemie cu un virus bizar, a cărui origine (naturală sau artificială) nu se cunoaște cu exactitate, care produce o infecție atipică, cu evoluție imprevizibilă, cu o multitudine de tablouri clinice, dar cu letalitate redusă, de numai 3,65%. Un betacoronavirus, numit SARS-CoV-2, care a apărut în noiembrie 2019, într-o piață de pește din localitatea chineză Wuhan, și care, printr-un complex de erori de gestionare a sinistrului, a ajuns să contamineze o lume întreagă, să închidă economiile marilor puteri și să anunțe, poate, finalul unui sistem și al unei

**Autoarea, expert în studii de securitate, este doctor în științe militare.*

ordini mondiale. Un sistem alcătuit din state și actori non-statali, asupra cărora pandemia a acționat nediscriminatoriu, lovind în punctele lor vulnerabile și amplificându-le. Și, o ordine mondială stabilită de matricea care unește toți acești actori, statali și non-statali, care, prin perturbările induse de pandemie, tinde să se reconfigureze. Evident, actorul principal al tuturor acestor transformări rămâne statul, descris generic prin patruleterul populație – teritoriu – idee națională – administrație, și analizat prin cinci dimensiuni: politică, economică, socială, ecologică și militară.

Prin urmare, acest articol dedicat analizei efectelor pandemiei de COVID-19 asupra sistemului internațional și ordinii mondiale urmărește să identifice impactul la nivel statal al crizei medicale globale, declanșate în noiembrie 2019.

Impactul politic intern al crizei medicale

Este binecunoscut faptul că, în primele luni de la debutul pandemiei, au existat mari deficiențe în gestionarea sinistrului atât la nivelul statelor, induse în eroare de comportamentul lipsit de transparență al Chinei și de ezitățile inexplicabile ale Organizației Mondiale a Sănătății (OMS) în privința naturii infecției și, mai ales, a severității ei², cât și la nivelul organizațiilor și instituțiilor internaționale, de la Uniunea Europeană (UE) la Organizația Națiunilor Unite (ONU)³. Informațiile contradictorii privind evoluția sinistrului au generat sincope în aprovizionarea cu materiale și echipamente medicale, au creat panică și sentimentul general al populației că guvernele sunt incapabile să țină situația sub control. Acest sentiment a fost, ulterior, combinat cu multitudinea de reacții negative induse de măsurile adoptate de guverne pentru limitarea focarelor epidemice, măsuri nepopulare care au inclus carantinarea populației, blocarea economiei, închiderea unor sectoare societale considerate a fi neesențiale funcționării statului, precum educația, cultura, activitățile sportive, turismul etc. Dacă, inițial, cetățenii au acceptat măsurile, considerând că, astfel, se va opri infecția și viața va reveni la normal, ulterior, criza prelungindu-se, au început să gliseze spre proteste și conflicte între

autorități și populație, situație înregistrată în mari orașe precum Sofia⁴, Belgrad⁵, Berlin⁶, Londra⁷, Tel Aviv⁸, Montreal⁹ etc. În plan politic, această stare de nemulțumire s-a proiectat, în principal, asupra partidului/coaliției de guvernământ¹⁰. În unele cazuri, cum este Franța, unde mișcarea „vestelor galbene” a respins și restricțiile guvernamentale pe fondul pandemiei¹¹, nemulțumirea s-a proiectat asupra întregului spectru politic. De asemenea, impactul economic al închiderii economiilor, tradus prin șomaj și sărăcirea păturilor vulnerabile ale societății, mai ales în condițiile unei crize prelungite, poate să amplifice frustrarea populară, crescând riscul exploziilor sociale.

Pe un astfel de fond, emergența liderilor și a partidelor noi, cu discurs populist, sau a partidelor conservatoare și suveraniste este greu de evitat. De altfel, primatul interesului național a fost vizibil, deja, în primele luni ale pandemiei, când statele europene au ignorat apelul de ajutor al Italiei și au preferat să închidă granițele și să se îngrijească de proprii cetățeni¹². În cazul unei crize medicale prelungite pe durata a doi sau mai mulți ani, dublate de o prăbușire politică a partidelor neoliberale și de o prăbușire economică a statelor, este posibil să asistăm la implozia societății globale neoliberale, urmată de reconfigurări și reasezări ale ordinii mondiale, cel mai probabil de natura multipolară.

Evident, există și riscul amplificării mișcărilor politice extremiste și anarhiste, care ar putea dinamita și mai rapid trama matricei neoliberale. Hrănite de ideologii totalitare, neomarxiste, aceste mișcări, în context pandemic, ar putea instrumentaliza politic nevoia combaterii infecției și s-ar putea îndrepta împotriva asimptomaticilor din grupele de populație vârstnică, mai conservatoare, transformându-i în ținte ale oprobiului public și marginalizării sociale. Deja, astfel de mișcări neomarxiste acționează în SUA, unde au drept țintă capitalismul conservator (Antifa¹³, Black Lives Matter¹⁴, Occupy Wall Street¹⁵).

Starea de incertitudine privind durata pandemiei, panica și nemulțumirea publică devin o mare vulnerabilitate, cu potențial subversiv, la adresa sistemului politic și a ordinii constituționale, cu atât mai mult cu cât ele pot fi alimentate ușor

de actori statali sau non-statali, interesați să submineze o putere statală, prin intermediul știrilor false – *fake news*. De altfel, sunt binecunoscute riscurile în planul securității naționale comportate de astfel de campanii de dezinformare, riscuri care pot culmina cu negarea existenței virusului, insubordonare civică și haos. Și, nu numai atât. Pe acest fond tensionat, alimentat de *fake news* menite să scadă încrederea populației în propriul guvern, pot prolifera mișcări secesioniste și autonomiste, precum cea din Catalonia, care și-a declarat deja independența și revenirea provinciei spaniole la statutul de republică¹⁶.

Și, nu în ultimul rând, în domeniul diplomatic, afectat la rândul-i de suspendarea sau restrângerea reuniunilor internaționale, este posibil să asistăm la o digitalizare extinsă, însoțită, evident, de o scădere a performanței, știut fiind că arta diplomatică este, înainte de toate, arta comunicării și a impresionării interlocutorului.

Impactul economic al crizei medicale

După o perioadă de panică bursieră generată de închiderea economiilor marilor puteri globale, începând cu 27 martie 2020 situația s-a stabilizat, prin intervenția financiară masivă a administrației Trump, care a instituit cel mai mare program de finanțare de urgență din istoria țării, intitulat *CARES Act*. Aprobând de ambele camere ale Congresului, programul, în valoare de 2.200 miliarde de dolari, a prevăzut ajutoare financiare nemaiîntâlnite în legislația americană, adresate populației vulnerabile, companiilor, îndeosebi celor mici și mijlocii, personalului medico-sanitar, Fondului de Ajutor pentru Dezastre, cercetării medicale¹⁷. De asemenea, în aceeași zi, Rezerva Federală a SUA a instituit măsuri economico-financiare de mare anvergură menite să îndepărteze riscul dispariției lichidităților din piață, precum scăderea la zero a dobânzii de referință, obligațiuni de stat emise de guvernul SUA, *liquidity swap lines* - linii de schimb de lichiditate foarte avantajoase și sigure pentru alte bănci centrale importante ale lumii, care au fost atrase să schimbe în cantități nelimitate propriile monede naționale cu dolari americani. În plus, s-a decis ca *Federal Open Market Committee* - *Comitetul Federal pentru Piața Deschisă*

(FOMC) să înceapă achiziționarea titlurilor de trezorerie și a titlurilor de stat ipotecate, în valoare de cel puțin 500 miliarde de dolari de valori mobiliare și cel puțin 200 miliarde de dolari în titluri ipotecare, inclusiv a valorilor mobiliare cu garanții ipotecare comerciale¹⁸, modalitate prin care a fost cumpărată, indirect, datoria marilor corporații americane.

Ulterior, și alte state au instituit măsuri economice de anvergură. De exemplu, China, care sărbătorește anul viitor, în 23 iulie 2021, centenarul Partidului Comunist Chinez, când trebuie raportată îndeplinirea obiectivelor legate de „Visul Chinei”, programul strategic care vizează întinerirea populației, „recuperarea suveranității asupra teritoriilor chineze pierdute prin impunerea unor tratate inegale de către puteri străine ostile”¹⁹ și dublarea valorii PIB (PPP) și a veniturilor pe cap de locuitor în deceniul 2010 – 2020. Programul, schițat încă din perioada președintelui Mao Zedong (1893-1976), vizează transformarea Chinei într-o putere hegemonică, pol al sistemului internațional. Prin urmare, imperativul combaterii efectelor economice ale pandemiei și al creșterii economice dobândește conotații aparte în acest context.

La rândul său, Federația Rusă a adoptat măsuri menite să susțină economia și, mai ales, populația vulnerabilă, în mare majoritate fără „perna financiară” capabilă să amortizeze șocul economic al pierderii locurilor de muncă²⁰. Între aceste măsuri se disting amânarea plăților pentru împrumuturi bugetare, compensații pentru pierderile suferite de bugetele regionale, amânarea colectării impozitelor pentru întreprinderile din cele mai afectate sectoare ale economiei, extinderea programului de împrumuturi *soft* (avantajoase), creșterea cuantumului subvențiilor pentru întreprinderile mici și mijlocii, facilitarea condițiilor de creditare pentru industriile afectate de coronavirus etc²¹.

Uniunea Europeană s-a confruntat cu mari divergențe legate de coronabonduri²² și de programul în valoare de 750 miliarde euro al Băncii Centrale Europene (BCE)²³. Dar, într-un final, au fost instituite programe economice și financiare menite să sprijine statele membre, precum pachetul de 540 de miliarde EUR alcătuit

din trei „plase de siguranță” financiară cu acțiune imediată pentru lucrători, întreprinderi și țările UE, sau redirecționarea fondurilor UE cu scopul de a ajuta statele membre în lupta contra pandemiei, fie fonduri structurale, fie fondul de solidaritate, fie sprijin de urgență de până la 40 de miliarde de euro pus la dispoziție de Banca Europeană de Investiții pentru a ajuta întreprinderile mici și mijlocii²⁴.

Cu toate acestea, economiile statelor lumii au intrat în recesiune. Cele mai mari pierderi s-au înregistrat în ramuri economice precum turismul, transporturile, în industriile primare, industria auto și de piese de schimb, industria cinematografiei, industriile de loisir și frumusețe, industriile de pielărie și confecții, industriile de aparatură electronică și electrocasnică etc., și în comerțul cu produse ne-esențiale vieții cotidiene. Conform datelor furnizate de Organizația Internațională a Muncii (OIM), la nivel mondial peste 436 de milioane de întreprinderi se confruntă cu mari riscuri de faliment. Dintre acestea, aproximativ 232 de milioane activează în comerțul cu ridicata și cu amănuntul, 111 milioane în industria prelucrătoare, 51 milioane în domeniul spațiilor de cazare și în servicii alimentare și 42 de milioane în domeniul imobieliarelor și în alte activități comerciale²⁵.

De fapt, recesiunea economică nu ar fi trebuit să reprezinte o surpriză, ea fiind anunțată de specialiști cu mult timp înainte, când atrăgeau atenția că economia mondială, interconectată și „supraîncălzită”, ascunde, de fapt, deficite structurale²⁶.

Conform Fondului Monetar Internațional (FMI), economia SUA ar putea suferi o contracție de 5,9 % în 2020, urmată de o creștere economică de 4,7 % în 2021, dacă nu va mai urma un alt val pandemic și o nouă închidere a economiei²⁷.

Tot prognozele FMI estimează că Zona Euro va scădea cu -7,5% în 2020 (cu o revenire în 2021 de +4,7%) și că vor exista contracții economice importante la nivelul principalelor economii europene, respectiv: Germania cu -7% (și posibilă revenire la +5,2% în 2021), Franța cu -7,2% (și +4,5% în 2021), Italia cu -9,1% (și +4,8% în 2021) și Spania cu -8% (și +4,2% în 2021)²⁸. De asemenea, conform aceleiași surse,

recesiunea economică a Federației Ruse, la finalul anului 2020, va atinge -5,5% în PIB (PPP)²⁹. Per ansamblu, 170 de țări ar putea intra în recesiune până la sfârșitul anului 2020, PIB-ul global urmând să scadă cu 3%³⁰, iar comerțul mondial de mărfuri urmând să sufere o contracție de 31,9%. Este considerată a fi cea mai puternică recesiune economică mondială, de la „marea recesiune” din decada 1929 – 1939 încoace.

Conform specialiștilor de la *Center for Macroeconomic Analysis and Short-term Forecasting (CMASF)* – Centrul de analiză macroeconomică și prognoză pe termen scurt, din Moscova, există trei scenarii posibile ale crizei economice induse de pandemie atât în Federația Rusă, cât și la nivel global:

– „*criza soft*”, care ia în calcul o evoluție de scurtă durată a pandemiei, cu o recuperare rapidă într-un an și revenirea la traiectoria pre-criză până în 2022 - cu o probabilitate de 15-17%;

– „*criza hard*”; de tip ciclic, pe durata a doi ani, cu o probabilitate de 55-57%;

– „*criza șoc*”, cel mai rău scenariu, aferent unei crize prelungite, care va duce la schimbări structurale durabile în economia rusă și globală, cu o probabilitate de 28-30%³¹.

Singurele mari economii creditate de FMI cu creștere economică, până la sfârșitul anului 2020, sunt cele ale Chinei, cu 1,2% (și o creștere în 2021 de +9,2%)³², și Indiei cu 1,9%³³.

Pe de altă parte, se remarcă o serie de transformări structurale ale economiilor statelor dezvoltate, începând cu dezvoltarea economiei intangibile și a economiei digitale, online. Giganții IT, precum *Alphabet*, *Amazon*, *Apple*, *Netflix*, *Facebook*, *Microsoft* și *Google*, au înregistrat creșteri spectaculoase ale cifrelor de afaceri (așa-numitele *FAAANG stocks*), prin utilizarea sporită de către utilizatori a platformelor digitale³⁴.

Nu același lucru se poate afirma, însă, în cazul statelor sărace, unde accesul la sistemele informatice este extrem de scăzut. În acest sens, dacă în cazul statelor dezvoltate efectele economice au fost amortizate de capacitatea de adaptare a operatorilor economici la cerințele unei economii digitalizate și de transferul unei părți importante din activitățile de servicii în mediul online, în cazul statelor sărace și subdezvoltate

efectele economice ale pandemiei au fost dramatice, întrucât au lovit în principalele surse de venit provenite din domeniul industriilor primare, extractive.

Astfel, putem spune că, *la nivel global, criza pandemică a adâncit discrepanțele economice dintre statele bogate și cele sărace, ultimele, dependente, încă din perioada prepandemică, de ajutor extern pentru supraviețuire.*

În acest sens, *Asian Development Bank* consideră că, în primele șase luni ale crizei, impactul economic global al pandemiei de COVID-19 poate atinge între 2000 – 4000 miliarde USD, iar *African Development Bank* estimează că pierderile economice ale Africii ar putea fi cuprinse între 22,1 – 88,3 miliarde USD, în timp ce datoria publică totală a continentului ar putea crește de la 1,86 trilioane USD, cât însuma la sfârșitul anului trecut, la peste 2 trilioane USD, în acest an³⁵.

Impactul social al crizei medicale

Actuala criză medicală a afectat toate cele trei dimensiuni ale bunăstării umane, respectiv:

- bunăstarea economică a populației, exprimată prin calitatea vieții;
- bunăstarea socială, exprimată prin nivelul libertăților individuale;
- bunăstarea civică și politică, exprimată prin participare în procesul deciziei politice și administrative din „cetate” și al exercitării puterii statale.

Potrivit Organizației Internaționale a Muncii, 305 milioane de locuri de muncă ar putea fi desființate ca urmare a pandemiei de COVID-19, iar 1,6 miliarde de lucrători din economia informală (cei mai vulnerabili economic, precum micii meseriași, micii comercianți, lucrătorii zilieri etc), reprezentând circa jumătate din forța de muncă globală, nu ar mai putea să-și asigure mijloacele de trai. Se estimează că prima lună a crizei medicale a determinat o scădere cu 60% a veniturilor lucrătorilor informali la nivel global, o scădere cu 81% în Africa și America, 21,6% în Asia și Pacific și 70% în Europa și Asia Centrală³⁶. La rândul său, United Nations Development Programme (UNDP) consideră

că în țările cu venituri mici și medii pierderile salariale vor depăși 220 de miliarde USD și că aproape jumătate din locurile de muncă din Africa ar putea fi pierdute. În cazul unei crize prelungite, guvernele statelor mici și mijlocii, confruntate cu spectrul incapacității de plată, ar putea recurge la curbe de sacrificiu, la suspendarea plății pensiilor și a salariilor personalului bugetar, la suspendarea finanțării pentru sectoare non-productive ale societății.

Toate aceste aspecte se traduc prin sărăcire accelerată și o scădere marcantă a calității vieții unor mari mase de oameni, chestiune care ar putea avea un impact major asupra mediului de securitate prin creșterea infraționalității, inclusiv a celei cu violență, intensificarea mișcărilor sociale de protest, nesupunere civică și insurgență, migrație ilegală transfrontalieră etc.

Și nu doar atât. Organizația Națiunilor Unite pentru Educație, Știință și Cultură (UNESCO) a afirmat că pandemia a determinat închiderea școlilor în 13 țări și a perturbat educația a 290,5 milioane de elevi și studenți la nivel global, ceea ce ar reprezenta o cifră „fără precedent”³⁷. Există opinii care susțin înlocuirea învățământului direct cu cel on-line, opinii dezavuate de numeroși specialiști în pedagogie³⁸, care reclamă lipsa interacțiunii din clasă, dintre profesor și elev, deficitul de socializare al elevilor, dar și probleme tehnice, legate de accesul la Internet al copiilor, accesul la mijloace computerizate, mai ales în țările sărace, disponibilitatea părinților de a supraveghea procesul educativ al copiilor etc.

Dar nu numai învățământul a fost profund perturbat, ci și activitățile culturale, sportive, confesionale, civice, interzise în perioada carantinării orașelor. Și, mai mult decât atât, au existat limitări ale drepturilor și libertăților cetățenești, care au afectat bunăstarea socială a indivizilor. În acest context, putem spune că, *una dintre marile provocări ale crizei medicale actuale o constituie stabilirea echilibrului între combaterea răspândirii infecției și respectarea, de către autorități, a drepturilor și libertăților fundamentale ale cetățenilor*, un subiect care va declanșa mari dezbateri și controverse în viitorul apropiat.

Cât privește bunăstarea politico-civică a indivizilor, criza medicală suprapusă peste perioade de alegeri (locale, parlamentare, prezidențiale) a afectat implicarea cetățenilor în campanii, a mutat centrul de greutate al campaniilor electorale de pe adunările electorale pe discursul televizat, înlocuind interacțiunea umană dintre candidat și electorat cu ecranul și difuzorul mass-media. Această distanțare socială și interpunere a tehnologiei în relația inter-umană nu se manifestă doar în planul vieții politice a individului, ci devine o constantă a vremurilor actuale, ale cărei efecte psihologice vor fi cuantificate în curând. Pentru că omul, ființă socială prin definiție, are nevoie de interacțiunea cu semenii săi pentru un bun echilibru psihic și fizic.

De departe, însă, cel mai încărcat sector social a fost cel al serviciilor de sănătate. Practic, pandemia de COVID-19 a descoperit limitele sistemelor naționale de asistență medicală la nivel mondial. Marele adevăr al gripei spaniole de acum 100 de ani a fost uitat de strategii și conducătorii acestei lumi și a trebuit să fie redescoperit în aceste luni scurse de la debutul infecției, cu pierderi de vieți omenești și cu mari consecințe economice. Adevărul este că, în fața unei avalanșe de îmbolnăviri, niciun sistem medical, oricât de performant ar fi, nu poate rezista, dacă nu există o pregătire prealabilă în privința stocurilor de materiale sanitare și medicale de urgență, dacă nu există protocoale de acțiune cu eficiență testată, dacă nu există cooperare și sprijin internațional, dacă nu există informații certe. S-a văzut acest lucru în Lombardia, unde funcționa cel mai performant sistem de sănătate din Italia, s-a văzut în Barcelona, s-a văzut în New York.

Pe de altă parte, actuala pandemie a readus în prim plan cercetarea științifică și, mai ales, cercetarea medicală. Privită mult timp, în state precum România, ca o „cenușăreasă”³⁹ - privată de fonduri și distrusă cu bună știință din rațiuni legate de competiția acerbă de pe piața medico-farmaceutică internațională - cercetarea medicală și-a dovedit, în aceste vremuri, importanța majoră și caracterul strategic, de apărare a populației împotriva agresiunii biologice de orice tip. În prezent, la nivel global, sunt alocate fonduri

masive de cercetare, fie pentru descoperirea unui vaccin menit să stopeze infecția, fie pentru obținerea unor medicamente eficiente în tratarea acesteia. Mai mult, se remarcă reaparitia competiției și a naționalismului tehnologic, specifice epocii ordinii bipolare, de data aceasta în privința vitezei cu care va fi elaborat primul vaccin contra coronavirusului. Competiție câștigată, se pare, de Federația Rusă, care a înregistrat primul vaccin anti-COVID-19⁴⁰. Dar, nu doar cercetarea medicală și-a demonstrat importanța, ci și cercetarea tehnologică și IT, sociologică și psihologică, implicate în producerea de echipamente și mijloace de transport specifice, în crearea aparatelor menite să identifice secvențele virale, în crearea de softuri capabile să stabilească prezența persoanelor infectate (*tracing applications*), în gestionarea tensiunilor sociale și prevenirea comportamentelor negative ale populației aflate sub stresul carantinării etc.

Și, nu în ultimul rând, criza medicală a testat solidaritatea umană și interstatală. Grija societății față de cei bătrâni și neputincioși, față de cei săraci și de cei bolnavi, față de lucrătorii medicali aruncați în lupta cu virusul fără echipamente de protecție, și-a demonstrat importanța și viabilitatea. Este suficient să amintim fondurile puse la dispoziția statelor în curs de dezvoltare de către marile instituții financiare internaționale și marile organizații de caritate⁴¹ sau sprijinul financiar, uman și material al instituțiilor ecleziastice (în cazul țării noastre, Biserica Ortodoxă Română⁴²) sau a organizațiilor civice, pentru diminuarea efectelor sinistrului.

Nu același lucru s-a remarcat în privința solidarității interstatale, cazul Italiei fiind deja amintit anterior. Practic, prin gravitatea și multitudinea efectelor asupra populației și prin totala concentrare a majorității statelor asupra propriilor provocări interne, criza medicală a demonstrat că, pe fond, societatea neoliberală, globalizată, fără granițe vizibile, a rămas doar un concept. *Testul globalizării a eșuat* pentru că este în firea societăților democratice să se întâmple astfel, de la Jean-Jacques Rousseau (1712-1778) încoace, între stat și cetățeni încheindu-se un contract social, prin care statul se obligă să reprezinte și să apere, înainte de orice, interesele de putere ale cetățenilor săi.

Impactul ecologic al crizei medicale

Pe termen foarte scurt, spre deosebire de celelalte sectoare societale, puternic afectate de criză medicală, mediul înconjurător pare a fi marele câștigător al acestei crize. În plan ecologic, închiderea economiilor marilor puteri și reducerea traficului aerian, terestru și maritim a determinat o scădere marcantă a poluării și o refacere accelerată a stratului de ozon al planetei, vizibilă din spațiu de pe stația orbitală⁴³. În 1-5 ani, însă, s-ar putea ca acest câștig să nu mai fie atât de mare. Afectate profund de recesiune, este puțin probabil ca statele să mai fie interesate să investească în producția de energie „verde”, scumpă și mai puțin eficientă, comparativ cu sistemele de producție clasice, bazate pe hidrocarburi și cărbuni. În aceste condiții, este posibil ca anumite programe, menite să limiteze emisiile de dioxid de carbon, să fie amânate.

Impactul militar al crizei medicale

Structurile de forță ale statelor, îndeosebi poliția și armata, au fost implicate activ în perioada „stării de urgență” în aplicarea măsurilor de control al focarelor de infecție. Dar, marile provocări este posibil să apară în viitorul apropiat, dacă statele vor reinstitui carantina, cu tot ce presupune acest aspect în plan economic și psihologic.

În contextul neîncrederii crescânde în OMS, pentru modul neprofesionist în care a gestionat primele luni ale pandemiei, și a existenței pe piață a unui vaccin intens contestat tocmai de OMS și de partenerii săi, este puțin probabil ca populațiile să mai accepte cu ușurință o nouă carantinare, crescând riscul izbucnirii protestelor, insubordonării civice, insurgenței. Pe de altă parte, sărăcirea populației amplifică atât riscurile amintite anterior, cât și riscul infraționalității și, mai ales, al infraționalității cibernetice și al celei cu violență. Starea de haos subrezește profund capacitatea de apărare a statului, vulnerabilizându-l în fața potențialelor amenințări externe.

Pe de altă parte, recesiunea economică și austeritatea bugetară, care se prefigurează pentru anii care vin, mai ales dacă această criză medicală

se va prelungi, ar putea limita investițiile în domeniul apărării, fiind posibil să asistăm la restrângeri de personal și/sau la suspendarea unor programe de înarmare și de cercetare în domeniul militar.

Concluzii

Este binecunoscut în literatura de specialitate faptul că arma biologică este supranumită *arma nucleară a săracului*. Însă, actuala pandemie a arătat că este mult mai mult decât atât. Capacitatea marilor epidemii/pandemii de a distruge state, de a destructura sisteme și de a reconfigura ordini mondiale, le transformă în vectori supremi care, întotdeauna, anunță o mare schimbare de paradigmă. Care va fi aceea? Va fi ea un socialism globalizat trans-umanist? Va fi o întoarcere a statelor la preceptele contractului social, în baza căruia există și funcționează? Rămâne de văzut.

Cert este că, sub impact pandemic, statele se clatină, solidaritatea dintre ele se năruie, economia se prăbușește, societatea se fragmentează și se ostilizează, iar instituțiile de forță devin mult mai vizibile.

În era digitală, interacțiunea umană este înlocuită cu interfața computerului. Computerizarea vieții de zi cu zi, de la contactul social la viața politică, învățământ, cultură, servicii medicale și religioase, aduce cu sine însingurarea individului, cu efecte psihologice greu de cuantificat.

Actuala pandemie de COVID-19 este un exercițiu a ceea ce ar putea fi, dacă omenirea nu îi înțelege resorturile și, mai ales, lecțiile. Ceea ce astăzi a produs un cutremur, mâine, în condițiile unei tulpini foarte agresive, ar putea produce un cataclism. Depinde doar de modul în care comunitatea internațională înțelege să penalizeze sever orice stat sau instituție globală de profil, care, o dată izbucnit un astfel de sinistru, alege să-l ascundă și, mai mult decât atât, îl răspândește, cu bună știință, în întreaga lume.

Până la urmă, și pandemiile au un început.

Și, dacă începutul acestora este abordat cum se cuvine, milioane și milioane de vieți sunt salvate.

- ¹ <https://www.worldometers.info/coronavirus/>, accesat la data de 09.08.2020.
- ² Jenny Lei Ravelo, Sara Jerving, „COVID-19 — a timeline of the coronavirus outbreak“, <https://www.devex.com/news/covid-19-a-timeline-of-the-coronavirus-outbreak-96396>, accesat la data de 13.04.2020.
- ³ Jenny Lei Ravelo, Sara Jerving, *Op.cit.*
- ⁴ Damian Vodenitcharov, Lauren Chadwick, „I’m ashamed of our rulers’: Bulgarians on why anti-government protests are continuing“, Euronews, 23.07.2020, <https://www.euronews.com/2020/07/23/i-m-ashamed-of-our-rulers-bulgarians-on-why-anti-government-protests-are-continuing>, accesat la data de 13.04.2020.
- ⁵ „Proteste violente în Serbia după ce președintele a luat decizia de a reimpune starea de urgență din cauza pandemiei“, Digi24, 08.07.2020, <https://www.digi24.ro/stiri/externe/proteste-violente-in-serbia-dupa-ce-presedintele-a-luat-decizia-de-a-reimpune-starea-de-urgenta-din-cauza-pandemiei-1334769>, accesat la data de 13.08.2020.
- ⁶ „Coronavirus rallies: Germany’s growing anti-lockdown movement“, DW, 06.08.2020, <https://www.dw.com/en/germany-protests-coronavirus/a-54456654>, accesat la data de 13.08.2020.
- ⁷ Mary Meisenzahl, „A protest in London drew hundreds of demonstrators to push back against UK mask requirements“, Business Insider, 19.07.2020, <https://www.businessinsider.com/protestors-demonstrated-against-mask-laws-in-hyde-park-london-2020-7>, accesat la data de 13.08.2020.
- ⁸ *Thousands in Israel protest Netanyahu’s coronavirus response*, France 24, 19.07.2020, <https://www.france24.com/en/20200719-thousands-in-israel-protest-government-s-coronavirus-response>, accesat la data de 13.08.2020.
- ⁹ „Thousands rally in downtown Montreal to protest Quebec’s mandatory mask rules“, CBC News, 08.08.2020, <https://www.cbc.ca/news/canada/montreal/anti-mask-march-montreal-aug-8-1.5679598>, accesat la data de 13.08.2020.
- ¹⁰ „De la crise des Gilets jaunes à celle du Covid-19, les étapes marquantes d’Édouard Philippe à Matignon“, La Voix du Nord, 03.07.2020, <https://www.lavoixdunord.fr/773047/article/2020-07-03/de-la-crise-des-gilets-jaunes-celle-du-covid-19-les-etapes-marquantes-d-edouard>, accesat la data de 13.08.2020.
- ¹¹ John Irish, „Coronavirus: French gilets jaunes defy lockdown“, *The Independent*, 14.03.2020, <https://www.independent.co.uk/news/world/europe/coronavirus-news-france-paris-lockdown-gilet-jaunes-a9402381.html>, accesat la data de 13.08.2020.
- ¹² „Just when Italy really needed some unity, the EU failed it – and continues to do so“, *The Guardian*, 19.04.2020, <https://www.theguardian.com/world/2020/apr/19/european-union-italy-unity-failure-debt-germany-netherlands>, accesat la data de 13.08.2020.
- ¹³ „What is Antifa?“, *Al Jazeera*, 02.06.2020, <https://www.aljazeera.com/news/2020/06/antifa-200601170721571.html>, accesat la data de 13.08.2020.
- ¹⁴ Ryan W. Miller, „Black Lives Matter: A primer on what it is and what it stands for“, USA Today, 08.08.2016, <https://eu.usatoday.com/story/news/nation/2016/07/11/black-lives-matter-what-what-stands/86963292/>, accesat la data de 13.08.2020.
- ¹⁵ „Measuring Occupy Wall Street’s impact, 5 years later“, *Chicago Tribune*, 17.09.2017, <https://www.chicagotribune.com/nation-world/ct-occupy-wall-street-s-impact-20160917-story.html>, accesat la data de 13.08.2020.
- ¹⁶ Raphael Minder, Patrick Kingsley, „In Catalonia, a Declaration of Independence From Spain (Sort of)“, *New York Times*, 10.10.2017, accesat la data de 13.08.2020.
- ¹⁷ *Remarks by President Trump at Signing of H.R. 748, The CARES Act*, White House, 27.03.2020, <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-signing-h-r-748-cares-act/>, accesat la data de 13.08.2020.
- ¹⁸ *Federal Reserve issues FOMC statement*, 23 March 2020, <https://www.federalreserve.gov/newsevents/pressreleases/monetary20200323a.htm>, accesat la data de 13.08.2020.
- ¹⁹ Jayadeva Ranade, „Xi Jinping is striving to achieve the ‘China Dream’“, 28.03.2020, *Sunday Guardian*, <https://www.sundayguardianlive.com/opinion/xi-jinping-striving-achieve-china-dream>, accesat la data de 01.08.2020.
- ²⁰ Maria Kotova, Dezan Shira, *The Social & Economic Impact Of Covid-19 On Russia And Recovery Potential*, Russia Briefing, 13.04.2020, <https://www.russia-briefing.com/news/social-economic-impact-covid-19-russia-recovery-potential.html>, accesat la data de 05.08.2020.
- ²¹ Maria Kotova, Dezan Shira, *Op.cit.*
- ²² Joe Barnes, „EU meltdown: Italy slams Merkel for lack of unity – Macron says coronavirus could end bloc“, *Express*, 28.03.2020, <https://www.express.co.uk/news/world/1261075/EU-coronavirus-summit-Italy-economy-Angela-Merkel-Emmanuel-Macron-collapse>, accesat la data de 11.08.2020.
- ²³ Pus în dificultate de decizia Curții Constituționale a Germaniei privind neconstituționalitatea parțială a participării *Bundesbank*, principalul finanțator al BCE, într-un Program de achiziție în Sectorul Public (PSPP), menit să salveze EuroZone, în martie 2015, și obligativitatea de a returna la bugetul de stat al Germaniei suma de 2100 de miliarde de euro. Vezi: Silvia Amaro, „Italy asks for help from EU crisis fund as death toll spikes“, *CNBC*, 20.03.2020, <https://www.cnn.com/2020/03/20/italy-conte-calls-for-eu-crisis-fund-as-coronavirus-death-toll-rises.html>, accesat la data de 11.08.2020.
- ²⁴ „The common EU response to COVID-19“, https://europa.eu/european-union/coronavirus-response_en, accesat la data de 13.08.2020.

- ²⁵ILO: As job losses escalate, nearly half of global workforce at risk of losing livelihoods, *International Labour Organization*, 29.04.2020, https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_743036/lang--en/index.htm, accesat la data de 05.08.2020.
- ²⁶Erik Sherman, „Why the Next Recession May Feel Very Different Than 2008“, *Fortune*, 02.09.2019, <https://fortune.com/2019/09/02/next-recession-different-2008-great-recession/>, accesat la data de 05.08.2020.
- ²⁷Real GDP Growth, IMF, https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/USA, accesat la data de 01.08.2020.
- ²⁸World Economic Outlook, „April 2020: The Great Lockdown, International Monetary Fund“, April 2020, <https://www.imf.org/en/Publications/WEO/Issues/2020/04/14/weo-april-2020>, accesat la data de 13.08.2020.
- ²⁹Real GDP growth, IMF, https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/OEMDC/ADVEC/WEOORLD/RUS, accesat la data de 07.08.2020.
- ³⁰Gita Gopinath, „The Great Lockdown: Worst Economic Downturn Since the Great Depression“, IMF Blog, 14.04.2020, <https://blogs.imf.org/2020/04/14/the-great-lockdown-worst-economic-downturn-since-the-great-depression/>, accesat la data de 07.08.2020.
- ³¹Maria Kotova, Dezan Shira, *idem.op.cit.*
- ³²Real GDP growth, IMF, https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/USA/CHN, accesat la data de 01.08.2020.
- ³³IMF projects India's growth rate at 1.9% in 2020 due to coronavirus“, *hindustantimes*, 14.04.2020, <https://www.hindustantimes.com/business-news/imf-projects-india-s-growth-rate-at-1-9-in-2020-due-to-coronavirus/story-KpKvxeSj9IIwf5kXnr0JcJ.html>, accesat la data de 05.08.2020.
- ³⁴Robin Wigglesworth, „How Big Tech got even bigger in the Covid-19 era“, *Financial Times*, 01.05.2020, <https://www.ft.com/content/d2e09235-b28e-438d-9b55-0e6bab7ac8ec>, accesat la data de 05.08.2020.
- ³⁵Jenny Lei Ravelo, Sara Jerving, „COVID-19 — a timeline of the coronavirus outbreak“, <https://www.devex.com/news/covid-19-a-timeline-of-the-coronavirus-outbreak-96396>, accesat la data de 13.08.2020.
- ³⁶„ILO: As job losses escalate, nearly half of global workforce at risk of losing livelihoods“, *idem.*, op.cit.
- ³⁷*Ibidem.*
- ³⁸„Academia Română: Educația online este o formă complementară educației directe, în sala de clasă“, *Agerpres*, 28.07.2020, <https://www.agerpres.ro/educatie-stiinta/2020/07/28/academia-romana-educatia-online-este-o-forma-complementara-educatiei-directe-in-sala-de-clasa--547029>, accesat la data de 13.08.2020.
- ³⁹Referire la personajul cu același nume din basmul „Cenușăreasa” al scriitorului francez Charles Perrault (1628-1703), în care fata transformată în cenușăreasă de mama vitregă, devine prințesa acelui regat.
- ⁴⁰„Sputnik V: What we know about Russia's coronavirus vaccine“, *Al Jazeera*, 13.08.2020, <https://www.aljazeera.com/news/2020/08/sputnik-russia-coronavirus-vaccine-200813070859021.html>, accesat la data de 13.08.2020.
- ⁴¹Jenny Lei Ravelo, Sara Jerving, *idem.op.cit.*
- ⁴²Otilia Serescu, Patriarhia: BOR a investit aproape 10 milioane de lei pentru combaterea efectelor provocate de COVID-19, *MediaFax*, 14.04.2020, <https://www.mediafax.ro/economic/patriarhia-bor-a-investit-aproape-10-milioane-de-lei-pentru-combaterea-efectelor-provocate-de-covid-19-19070972>, accesat la data de 13.08.2020.
- ⁴³„Air pollution goes down as Europe takes hard measures to combat coronavirus“, *European Environment Agency*, 25.03.2020, <https://www.eea.europa.eu/highlights/air-pollution-goes-down-as>, accesat la data de 13.08.2020.

EFECTELE PANDEMIEI DE COVID-19 ÎN SPAȚIUL CIBERNETIC

Constantin NILĂ*
Marius PREDA
Cornel ARGINT

Abstract

The strong emotional reaction generated by the COVID-19 pandemic led to a significant increase in public interest in the subject. The most common searches on the Internet revolve around the virus spread, the ways of infection and the methods used for prevention. Consequently, the active threat actors from the cyberspace took advantage of the changes that occurred in the population lifestyle by exploiting the inadequate or non-existent security measures, especially in the context of the unanimous work from home policy. Organizations must not only respond to cyber-attacks by identifying and mitigating vulnerabilities, but also be able to recover from them. This article addresses the trends observed in cyberspace in the pandemic context, the major changes seen in the modus operandi of the attackers and the response of the authorities.

Keywords: coronavirus, COVID-19, SARS-CoV-2, cyberattack, cyber security.

1. Introducere

Impactul produs de pandemia de COVID-19 nu este încă pe deplin cunoscut și evaluat. Fiind una dintre cele mai grave pandemii din ultimul secol, boala produsă de agentul patogen SARS-CoV-2 a schimbat radical modul în care cetățenii interacționează unii cu alții, își desfășoară activitatea și percep societatea. Aceștia asistă, din poziția de martori, la o schimbare majoră atât pe plan național, cât și internațional, contextul geopolitic modificându-se mai repede ca niciodată.

În acest context, a fost observată o accentuare a utilizării pe scară largă a infrastructurilor IT atât pentru desfășurarea activității, cât mai ales pentru asigurarea unor servicii esențiale precum controalele medicale periodice, învățământ, servicii comerciale sau procese financiar-economice. Măsurile impuse de autorități pentru limitarea efectelor pandemiei au forțat multe

companii să implementeze lucrul de acasă al angajaților. Prin urmare, au apărut o serie de probleme noi generate de faptul că organizațiile nu aveau infrastructura pregătită pentru lucrul de la distanță, iar stațiile personale de lucru ale angajaților nu aveau sisteme de securitate cibernetică la nivelul existent în rețeaua internă a companiei.

De asemenea, obligația de a sta în casă, inclusiv pentru copii, a condus la creșterea semnificativă a timpului petrecut în fața calculatorului sau telefonului. Acest lucru a avut ca efect direct atât accesarea mai multor resurse de informare pe Internet, cât și descărcarea unui număr mai mare de aplicații, fapt ce a condus la creșterea suprafeței de expunere la atacuri cibernetice.

Aceste vulnerabilități nou apărute au fost exploatate cu promptitudine de actori malițioși. Încă de la începutul anului 2020 s-a observat o

*Autorii sunt experți în cadrul Ministerului Apărării Naționale

creștere a intensității atacurilor cibernetice, în unele cazuri bunele practici de securitate cibernetică dovedindu-se ineficiente și depășite pe fondul forțării organizațiilor în a utiliza tehnologii noi, netestate, pentru asigurarea serviciilor în noile condiții de pandemie.

Actorii statali au fost implicați cu preponderență în acțiuni de spionaj cibernetic, orientate spre obținerea de informații despre măsurile de combatere a virusului SARS-CoV-2, potențiale rezultate ale testărilor de vaccine și opțiuni de tratament. Pentru descurajarea acestora, activitățile sponsorizate de stat au determinat în unele cazuri impunerea de sancțiuni politice și economice [5].

Actorii non-statali au condus campanii cu impact semnificativ asupra infrastructurilor cibernetice, aceștia vizând orice interacțiune cu tehnologia pentru obținerea unui avantaj de natură financiară. Email-ul a fost și va continua să fie cel mai utilizat vector de atac, atât pentru cetățenii de rând, cât și pentru organizații. Actorii malițioși din spațiul cibernetic au utilizat de mult timp evenimente majore și larg mediatizate în campaniile de phishing pentru a spori eficiența atacurilor lor, pandemia actuală nefiind decât o nouă oportunitate majoră pentru a le spori șansele de succes [6].

Bunele practici de securitate cibernetică s-au dovedit ineficiente și depășite din momentul în care organizațiile au implementat tehnologii noi, netestate, pentru asigurarea serviciilor [4]. De exemplu, implementarea lucrului de la distanță a introdus două riscuri noi de securitate:

1. deschiderea mai multor servicii sau porturi la Internet decât în cazul lucrului în rețeaua închisă de la birou;
2. politicile de securitate stabilite pentru stația de lucru de la domiciliu sunt mai slabe decât cele de la birou, acestea nefiind adaptate pentru derularea activității online.

Ca urmare, securitatea cibernetică a căpătat o importanță tot mai crescută, spațiul cibernetic mutându-se în centrul atenției în era distanțării fizice și a presiunii constante create de pandemia de COVID-19.

2. Schimbări în spațiul cibernetic impuse de pandemie

2.1. Evoluția campaniilor de phishing

În data de 31 decembrie 2019, noul coronavirus SARS-CoV-2 a ajuns în atenția globală, China raportând către Organizația Mondială a Sănătății (OMS), pentru prima dată, un număr de cazuri de pneumonie, înregistrate în Wuhan, provincia Hubei. Pe 16 ianuarie 2020, China a început adoptarea de măsuri pentru izolare. Paisprezece zile mai târziu, OMS a declarat situație de urgență de natură internațională în domeniul sănătății publice (PHEIC), iar în data de 31 ianuarie 2020 primele cazuri de COVID-19 au fost raportate în Europa. După numai trei săptămâni (21 februarie 2020) au avut loc primele prăbușiri ale piețelor bursiere atribuite extinderii epidemiei.

Modelul grafic de răspândire a virusului în lume a fost urmat fidel de atacurile desfășurate în spațiul cibernetic, infractorii din acest mediu exploatând din plin atât curiozitatea populației față de noul fenomen, cât și vulnerabilitățile apărute ca urmare a implementării rapide a unor tehnologii noi, insuficient testate din punct de vedere al securității cibernetice.

În timp ce întreaga lume lupta împotriva COVID-19, actorii din spațiul cibernetic au considerat pandemia oportună pentru derularea unor atacuri în masă, în scopul însușirii rapide de active financiare. Criminalitatea cibernetică

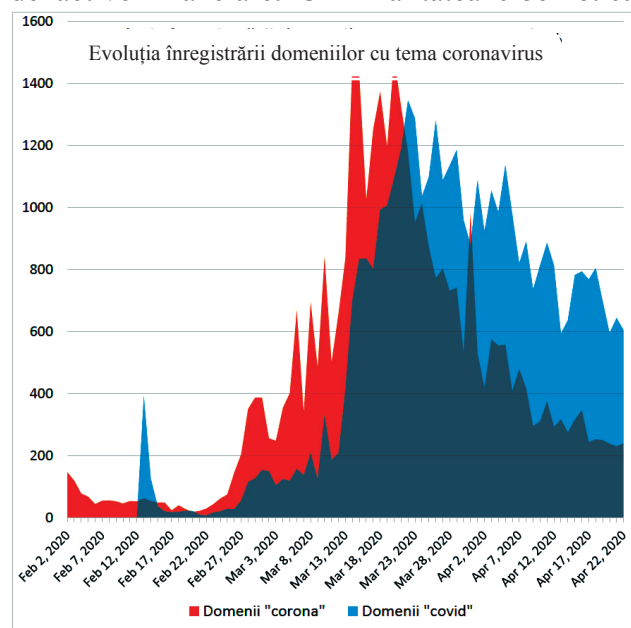


Figura 1 - Tendințe de înregistrare domenii cu tema COVID-19

a beneficiat din plin de sentimentul de insecuritate manifestat în rândul populației și de nevoia de informare a oamenilor [5].

În timp ce în luna martie tot mai multe state luau măsuri drastice de izolare pentru suprimarea pandemiei, specialiștii IBM X-Force au raportat o creștere cu 6.000% a mesajelor de tip spam care exploatau tema coronavirus [2] [3].

În același timp, într-un raport [8] publicat de compania Google, în luna aprilie, este subliniată o creștere la 18 milioane de e-mail-uri pe zi care conțineau malware deghizat în subiecte cu tema COVID-19. Similar, compania Mimecast Threat Center a analizat, din ianuarie până în iunie 2020, mai mult de 195 de miliarde de e-mail-uri doar în SUA și regiunea Caraibe, 92 de miliarde (47%) dintre acestea având conținut malițios [7]. Atacurile din această categorie au exploatat sentimentul de teamă și au oferit ca momeală stimulente financiare, cu scopul de a compromite victimele.

Echipele de răspuns la incidente de securitate cibernetică (CSIRT) din cadrul UE au identificat multiple campanii de phishing cu tema COVID-19, unele dintre ele traduse în limba locală, utilizând nume de domenii similare cu cele ale Organizației Mondiale a Sănătății, Centrului pentru Controlul Bolilor din SUA și altele [9].

Tot de la începutul anului 2020 a fost identificat un nou mod de operare utilizat în atacurile cibernetice. Acesta constă în efectuarea unui apel telefonic către victimă concomitent cu transmiterea mesajului de phishing, pentru a convinge victima să acceseze mesajul, crescând semnificativ rata de succes a atacurilor. În contextul dependenței crescute a populației de serviciile poștale și de livrări, generată de criza actuală, a crescut semnificativ numărul fraudelor care exploatează identitatea companiilor de livrări. La nivel internațional au fost identificate campanii de spam care impersonau DHL, UPS, FedEx și alte entități din acest sector.

Din analiza numelor de domenii înregistrate (figura 1), în perioada ianuarie-mai au fost observate aproximativ 76 de mii de domenii cu denumiri conexe sau derivate din COVID-19. Domeniile similare cu cele publice sunt ușor de falsificat și contribuie la creșterea probabilității și a impactului atacurilor cibernetice.

De asemenea, a fost observată înregistrarea domeniilor care conțin greșeli gramaticale, dar care seamănă cu cele utilizate de companii precum Zoom, Webex, Google Hangouts și Houseparty, serviciile acestora fiind utilizate în activitatea de la domiciliu. După înregistrare, paginile web au fost menținute o perioadă fără conținut și activate doar în momentul desfășurării campaniilor malițioase.

Pe fondul răspândirii pandemiei de COVID-19 în Europa și America, în perioada martie-aprilie a fost atins un nou vârf absolut al atacurilor cibernetice. În această perioadă, a fost înregistrată o creștere semnificativă a agresiunilor la nivel global, estimată la 600% față de o perioadă de referință normală. Atacurile cibernetice au vizat cu preponderență serviciile medicale, domeniul educației, mass media, domeniul publicitar și domeniul hotelier. Majoritatea atacurilor cibernetice au fost îndreptate împotriva următoarelor state: Italia, Cehia, Japonia, SUA, Canada, Australia și Turcia.

Este important de evidențiat faptul că atacatorii au lansat campanii simultane de atac cibernetic împotriva unui număr mare de ținte. Popularitatea așa-numitelor servicii de tip Malware-as-a-Service (MaaS) a crescut în rândurile actorilor malițioși, cel mai cunoscut serviciu din această perioadă fiind Emotet, care a fost utilizat pentru distribuirea de ransomware și malware de tip backdoor/infostealer [7]. Actorul din spatele Emotet oferea servicii de distribuire malware, cum ar fi TrickBot, Ryuk și Dridex, utilizând subiecte cu tema COVID-19 pentru pivotarea atacurilor din primele faze ale crizei (ianuarie 2020). Acest exemplu a fost urmat ulterior și de alți actori, fapt care a condus la crearea a sute de mii de email-uri de phishing cu temă coronavirus [4].

2.2. Atacuri asupra soluțiilor de lucru de la distanță

Din datele publice, numărul familiilor de malware care utilizează tematica COVID-19 în atacuri cibernetice a crescut rapid în luna martie și în prima parte a lunii aprilie a acestui an. La începutul celui de-al doilea semestru al anului 2020, au fost identificate aproximativ 80 de familii malware care utilizează pandemia pentru a-și infecta victimele [9].

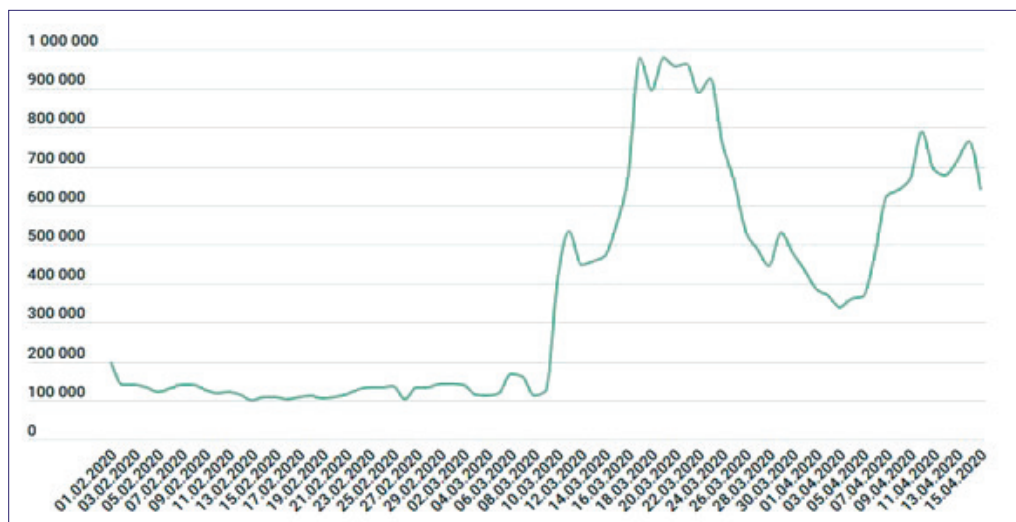


Figura 2 - Evoluția atacurilor RDP în perioada 01.02 - 15.04.2020

Totodată, încă de la începutul pandemiei de COVID-19 a fost observată o accentuare a numărului atacurilor asupra tehnologiilor specifice lucrului de la distanță, prin utilizarea unor mijloace care nu erau testate suficient. Vulnerabilitatea a fost generată de faptul că majoritatea organizațiilor publice și private au început să adopte mecanisme de lucru de la distanță pentru a limita răspândirea noului coronavirus în rândul angajaților și pentru a asigura continuitatea activității.

Din punct de vedere tehnic, acest lucru a fost reflectat în creșterea numărului de sisteme informatice care au portul 3389¹, vizibil în Internet. Această creștere s-a observat la nivel global începând cu luna ianuarie 2020, dar s-a accentuat începând cu luna februarie, când pandemia a început să se răspândească și în Europa. Atacurile care au exploatat vulnerabilitățile acestui protocol au crescut de aproape 10 ori în intensitate odată cu generalizarea modelului de lucru de acasă (la jumătatea lunii martie), pe fondul răspândirii pandemiei și a impunerii unor restricții severe de circulație a persoanelor (figura 2).

Soluția alternativă implementată de administratorii de securitate, de a utiliza un protocol sau un port diferit de acces de la distanță, nu a constituit o piedică pentru atacatori. Astfel, în cursul anului 2020 au fost descoperite 37 de vulnerabilități numai în aplicațiile care utilizează un protocol alternativ - VNC (Virtual Network Computing).

O altă țintă importantă pentru atacatori a fost reprezentată de Sistemele de Control Industrial

(SCADA). Deși numărul dispozitivelor SCADA vizibile în Internet nu este semnificativ, acestea prezintă un risc ridicat prin faptul că pot controla procese critice (instalații energetice, de distribuire a apei potabile etc.) și nu dispun de sisteme de autentificare și de securitate adecvate. În prima parte a acestui an, a fost observată o creștere cu 16% a numărului de sisteme informatice din domeniul SCADA vizibile în Internet, posibil pentru a permite controlul acestora de acasă.

Potrivit unei analize realizate de către specialiștii companiei Bitdefender[11], începând cu luna octombrie a anului 2019, interesul actorilor din spațiul cibernetic privind industria de petrol și gaze a crescut progresiv. Campaniile identificate au fost amplificate de actuala criză sanitară, obiectivul acestora fiind culegerea de informații din sistemele informatice de interes, pe fondul negocierilor OPEC (Organizația Țărilor Exportatoare de Petrol).

2.3. Supravegherea populației prin intermediul aplicațiilor mobile

O altă schimbare de amploare survenită pe fondul pandemiei a fost reprezentată de implementarea tehnologiilor pentru monitorizarea persoanelor infectate cu SARS-CoV-2, ca măsură alternativă de limitare a pandemiei. Cele mai multe aplicații dezvoltate în această direcție s-au bazat pe urmărirea telefoanelor mobile ale persoanelor infectate. În cele mai multe cazuri, s-a urmărit identificarea persoanelor care au intrat în contact cu subiecții infectați, prin monitorizarea canalelor de comunicație WiFi și bluetooth.

Numărul țărilor care au luat în considerare sau care au implementat tehnologii de supraveghere a crescut brusc în prima jumătate a lunii aprilie. Ulterior, tot mai multe țări au luat în considerare adoptarea unor astfel de soluții, astfel încât, în luna iunie, cel puțin 54 de țări dispuneau de tehnologii de supraveghere a interacțiunilor dintre cetățeni.

Profitând de supremația pe piață, Apple și Google au anunțat în luna mai lansarea tehnologiei pentru urmărirea contactelor persoanelor infectate. Soluțiile dezvoltate de cele două companii utilizează conexiunile Bluetooth dintre dispozitivele mobile pentru a identifica utilizatorii care se află într-o proximitate fizică timp de cel puțin cinci minute cu persoanele identificate. Deoarece aplicațiile pot avea dublă utilizare, cele două companii au interzis autorităților să le folosească pentru a colecta date privind locația sau pentru a cere utilizatorilor să introducă date personale [10].

Aceste aplicații pot fi exploatate de atacatori pentru monitorizarea anumitor persoane de interes sau furt de date. În luna aprilie a fost raportată o versiune malițioasă a aplicației SoftMining's SM_Covid19, dezvoltată inițial pentru monitorizarea interacțiunii dintre dispozitivele mobile, distanțării sociale și, respectiv, estimarea ratei de răspândire a virusului SARS-CoV-2. Ulterior, au fost descoperite în magazinul oficial GooglePlay alte 11 versiuni care conțineau aplicații malițioase din suita Metasploit.

Concluzii

Pandemia de COVID-19 a produs multe schimbări în societatea contemporană. Principalul efect în spațiul cibernetic a constat în forțarea digitalizării, multe organizații fiind obligate să-și regândească activitatea prin migrarea către activitatea de la distanță și prioritizarea operațiunilor de afaceri. Concomitent, aceste schimbări în spațiul cibernetic au generat noi provocări și riscuri de securitate induse de noua paradigmă.

Sectorul cel mai vizat de atacuri cibernetice a fost cel medical atât actorii statali, cât și cei non-statali fiind atrași de tehnologia învechită utilizată în cadrul instituțiilor medicale, de faptul că

acestea sunt mai înclinate să achite recompensele solicitate, pe fondul presiunii la care sunt supuse în această perioadă. Alte sectoare publice vizate în contextul pandemiei, în special de atacuri de tip DDoS și ransomware, au fost administrația, finanțele publice, cel energetic și educația.

Tehnologiile cele mai vizate de atacuri cibernetice au fost cele pentru facilitarea telecomunicării (aplicații de videoconferințe, chat și VPN). Aceste noi modalități de lucru au adus noi riscuri, astfel că sistemul actualizat de bune practici de protecție e-mail și securitate web au devenit esențiale. Controalele de securitate nu au putut fi aplicate sistemelor sau instrumentelor noi care au fost implementate în grabă pentru a sprijini angajații cu mijloace de lucru de la distanță (ex. Zoom). Ca urmare, educația și cultura de securitate cibernetică au rămas principalele măsuri de prevenire a amenințărilor de securitate cibernetică în noul context.

Riscurile aferente noului context au fost generate, în primul rând, de lipsa unui plan de răspuns adecvat. Conform unui raport din 2019 [2], 76% dintre instituții nu dispuneau de un plan de răspuns la incidente implementat în mod constant în întreaga organizație. Planurile de gestionare a crizelor trebuie să fie adaptate în funcție de natura și sfera amenințării, tipul și dimensiunea unei organizații și cerințele de reglementare în vigoare.

Deși scenariile care trebuie luate în considerare pentru asigurarea rezilienței operaționale sunt destul de ample, cel puțin în situații excepționale, cum este cel al pandemiei de COVID-19, ar trebui să fie luate în considerare îndrumările autorităților din domeniu pentru atingerea obiectivului de asigurare a unei rezistențe operaționale a întregii infrastructuri IT.

Totuși, pandemia actuală a avut și un efect benefic asupra lumii digitale, accelerând procesul de transfer al activităților în spațiul cibernetic. Sectoarele industriale de producție și IT au beneficiat de o creștere din punct de vedere economic [3]. Aceste creșteri au fost determinate de adaptabilitatea forței de muncă spre soluțiile digitale, utilizând la maxim suportul tehnologiilor actuale pentru a migra către munca de la distanță [4].

Pe fondul menținerii unui număr mare de persoane infectate cu SARS-CoV-2, estimăm că atacurile cibernetice care exploatează acest subiect vor continua să crească. Cel mai probabil, actorii din spațiul cibernetic vor continua să reprezinte o amenințare majoră și vor desfășura în continuare atacuri bazate pe tehnicile, tacticile și procedurile deja testate împotriva țintelor vulnerabile, exploatănd starea de confuzie indusă de noua paradigmă [4].

Bibliografie:

1. R. COELHO and J. Prenio, „FSI Briefs No. 2 - Covid-19 and operational resilience: addressing financial institutions’ operational challenges in a pandemic,” Financial Stability Institute, Aprilie 2020.
2. W. WHITMORE and G. Parham, „COVID-19 cyberwar: How to protect your business,” IBM Institute for Business Value, Iunie 2020.
3. “100 Days of Coronavirus (COVID-19)”, Mimecast, Mai 2020.
4. “Managing the impact of COVID-19 on cyber security,” pwc, Martie 2020.
5. J. WIGGEN, “The impact of COVID-19 on cyber crime and state-sponsored cyber activities”, Konrad Adenauer Stiftung, Iunie 2020.
6. “COVID-19: Cyber Threat Analysis”, United Nations Office on Drugs & Crime, Mai 2020.
7. „Threat Intelligence Report - Black Hat USA Edition 2020”, Mimecast, 2020.
8. “Creating a secure email ecosystem and blocking COVID-19 cyberthreats in India, Brazil and the UK”, Google, Aprilie 2020.
9. CERT-EU, 2020, <https://cert.europa.eu/> [Accesat 2020].
10. “How Apple and Google Are Enabling Covid-19 Contact-Tracing”, WIRED, Aprilie 2020.
11. „Atacatorii informatici profită de criza petrolului pentru a spiona companii din energie”, Bitdefender, Aprilie 2020.

¹ Portul 3389 - Remote Desktop Protocol (RDP) reprezintă un port utilizat de majoritatea aplicațiilor pentru desfășurarea de la distanță a unor activități pe sistemul informatic.

CAUZELE MANIPULĂRII INFORMAȚIILOR DE LA NIVELUL INDIVIDULUI

*Ilie CRISTIAN**

Abstract

Modern society is under constant information assault which determines its reactions, approaches, and behaviors. Taking advantage of human predisposition, encrypted on the complexity of the social world, the producers of information make use of complex mechanisms to inoculate desirable meanings.

The absence of cognitive discernment criteria and the tendency to assume the information that confirms our pre-existing hypothesis put us in dependence to cognitive biases and more and more to fake news.

Keywords: *modern society, information, bias, vulnerability, conspiracy theory, information manipulation, deception, fake news.*

Epoci și spații culturale diferite au explicat atât modul în care gestionăm problemele inteligibilității lumii în care trăim și acționăm, a structurilor instituționale, cât și relativismul contemporan al raționalității rezonabile.

Explorăm cauzele manipulării informațiilor, care rezidă parțial la nivelul individului, deoarece acestea sunt legate de natura umană și își găsesc, fără îndoială, rădăcinile în psihologie și epistemologie. Cauze există, fără rezervă, și la nivel colectiv, deoarece manipularea informațiilor este legată de viața noastră socială, de criza încrederii în instituții, în presă și de deziluziile cotidiene.

Domeniul manipulării informațiilor este saturat de o mulțime de termeni, care întrețes noțiuni clasice (influență, propagandă, dezinformare) cu neologisme (fakenews, post-adevăr etc.) a căror multiplicare arată complexitatea lumii sociale, care este într-o transformare completă.

Combaterea eficientă a manipulării informațiilor necesită identificarea originilor problemei, legate de natura umană, și implicit de psihologie și epistemologie (Ellul, J. 2017).

Dezinformarea exploatează o „lejeritate” intelectuală, naturală, caracterizată prin eșecul de a exercita în mod sistematic gândirea critică, dar și prin modul naiv de a alege informații, fără a căuta dovezi care să le susțină (Ellul, J. 2017).

Tindem, cel mai adesea, să favorizăm informațiile care confirmă ipotezele noastre preexistente, care sprijină pozițiile noastre anterioare și, totodată, nu ne ofensează sensibilitățile noastre (Ellul, J. 2017).

Acest fenomen psihologic este denumit, în mod obișnuit, „bias” de confirmare. În domeniul publicității, această sincopă este binecunoscută și exploatată, întrucât succesul unei campanii publicitare se întemeiază pe angajamentul și statornicia unui individ, adică pe tendința individului de a rămâne credincios unei opinii care este deja formată (Davis, J.J. 2011). În plus, noi toți avem tendința de a ne supraestima propriile noastre capacități de memorie și raționament și de a crede că suntem mult mai raționali și mai inteligenți decât suntem cu adevărat. În acest context, ideea cunoscută pe scară largă că raționamentul trebuie să fie imparțial și obiectiv

**Autorul este expert în cadrul Ministerului Apărării Naționale.*

și că acesta funcționează pentru a căuta adevărul este falsă (H. Mercier and D. Sperber, 2017). După cum scrie P. Engel (2018), „raționamentul nu a evoluat pentru a stabili realitatea, ci doar pentru a câștiga împotriva adversarilor noștri”.

Manipularea informațiilor este la fel de naturală ca vulnerabilitățile specifice naturii umane. În acest sens, un studiu recent (Vosoughi, Roy, Aral, 2018) a arătat că știrile false se răspândesc mai repede decât știrile exacte, din cauza unor motive psihologice. Știrile reale, adesea, nu constituie o noutate, sunt de obicei doar o confirmare a ceea ce deja știm sau suspectăm. Ele se adaugă, ca informații, la suma deja acumulată de cunoștințe și apoi sunt uitate rapid, în contrast cu surprizele știrilor false, care sunt scrise pentru a impresiona și pentru a merge împotriva rațiunii. Aspectul de noutate al știrilor false nu numai că provoacă un interes mai mare, dar explică, de asemenea, difuzarea lor, mult mai mare, de către cei care vor să-i uimească pe alții, adesea pentru creșterea reputației și a status-ului social.

În plus, știrile false sunt special adaptate pentru a se răspândi viral. Acestea sunt scrise într-un stil spectaculos, emoțional și adesea alarmist, luând în considerare impactul probabil al fricii și anxietății, elemente care nu sunt, în general, prioritare în domeniul știrilor reale. Prin urmare, prejudecățile noastre sunt cele care contribuie, în mare măsură, la răspândirea de știri false.

Cercetarea în domeniul publicității a identificat deja câteva „eșecuri” cognitive pe care o persoană calificată le poate exploata: nevoia de coerență a individului (biasul de confirmare); validarea prin interacțiune socială (individul va face ceea ce crede că fac alții); argumentul autorității (individul tinde să respecte dezerdatele autorității, chiar și atunci când i se solicită realizarea unor acte condamnabile); iluzia corelației, perceperea unei conexiuni între două evenimente, doar pentru că au avut loc într-un interval de timp apropiat; sau iluzia preferinței – o anumită opțiune este preferată deoarece persoanele sunt ușor de convins de oamenii pe care îi admiră (S.Vosoughi, D.Roy, S.Aral, 2018).

Manipularea informațiilor este doar una dintre manifestările unui fenomen mult mai mare, care integrează revizionismul istoric și teoriile conspirației.

Scriitorul și jurnalistul britanic D.Thompson (2018) a avertizat publicul despre existența unei „pandemii” de gândire naivă și despre declinul valorilor Iluminismului în fața non-științei. Faptul este că acum ne confruntăm cu o situație în care o mare parte din populație trăiește într-un spațiu epistemic care a abandonat criteriile convenționale de analiză, precum dovezile, coerența internă și căutarea de fapte. Rezultă că starea discursului public nu mai poate fi examinată prin intermediul obiectivității și că dezinformarea poate fi percepută ca o realitate alternativă, care este împărțită de milioane de oameni.

Sociologul G. Bronner vede acest lucru ca rezultat al unei combinații a două elemente (Lewandowsky, Ecker, Cook, 2017). Pe de o parte, liberalizarea pieței de informații, în care sursele raționale trebuie să concureze cu sursele iraționale; în acest sens, de reținut este faptul că această concurență favorizează credulii care sunt, în general, mai motivați decât „raționali” să-și apere punctul lor de vedere și să-i dedice timp pentru a-l susține (G.Bronner, 2013). Iar, pe de altă parte, el observă „lenea”, descrisă ca fiind de fapt lejeritatea intelectuală a utilizatorilor de media, care suferă de diferitele prejudecăți cognitive, inclusiv de bias-ul de confirmare. Pentru Olivier Schmitt, criza epistemologică actuală provine din împletirea, în spațiul public, a trei variante falsificate ale unor abordări epistemologice.

Prima abordare epistemologică, care este utilizată într-o formă contrafăcută, este îndoiala carteziană „cogito ergo sum”. Adică este transformată într-o îndoială sistematică, doar pentru a alimenta teoriile conspirației. A doua variantă de abordare epistemologică falsificată este relația dintre cunoaștere și putere: și aici îl cităm pe Foucault, care afirmă că de toate cunoștințele fabricate beneficiază, în mod inerent, cel mai puternic. Iar a treia variantă de abordare epistemologică falsificată este deconstructivismul, o abordare care, conform scrierilor lui Derrida, deschide posibilități

nelimitate interpretării. În varianta falsificată, deconstructivismul are drept scop deconstrucția sistematică a unui discurs dominant.

În ansamblu, criza epistemologică contemporană constă în interpretarea voit greșită, deturnarea și simplificarea abordărilor legitime.

La începutul anilor 1960, filozoful Karl Popper și-a prezentat teoria conspirației. Potrivit acestei teorii, există o viziune conform căreia explicația oricărui tip de fenomen social constă în a afla cine este interesat de apariția aceluia fenomen. Deci, aproape tot ceea ce se întâmplă în societate - mai ales fenomene precum războiul, șomajul, sărăcia, lipsurile, pe care oamenii, de obicei, nu le acceptă, - este rezultatul dorinței și acțiunii directe a unor persoane și grupuri puternice.

Teoriile conspirației amplifică o tendință naturală pe care o avem, adică de a crede că orice efect este cauzat de acțiunea intenționată, în special acele defecte care sunt benefice anumitor persoane. Din acest motiv, există teoriile conspirației - acestea sunt inevitabile și se hrănesc în cea mai mare parte cu crize și evenimente violente.

Din fericire, nu toate teoriile conspirației sunt periculoase. Unele sunt inofensive. Dar altele pot avea efecte destabilizatoare, chiar dacă sunt împărtășite doar de un procent foarte mic al populației, atâta timp cât această mică minoritate este gata să ia măsuri violente. Cei mai mulți „consumatori” ai conspirațiilor nu sunt iraționali, ci pur și simplu le lipsesc sursele bune de informații. Iar teoriile pe care le apără sunt justificate în lumina informațiilor disponibile, dar nu în funcție de toate sursele care există și care pot fi consultate, ceea ce face ca argumentele lor să le pară plauzibile.

Cauza acestei probleme este sărăcia epistemică a mediilor lor. Această explicație este, de asemenea, valabilă și pentru extremism, în general, despre care unii autori spun că suferă de o „epistemologie deformată”. Prin urmare, una dintre soluții este „infiltrarea cognitivă” cu intenția să se semene îndoieli și neîncredere în mintea indivizilor prin introducerea unei diversități de explicații (R.Hardin, 2002).

Teoriile conspirației prezintă o particularitate neobișnuită - sunt foarte puternice, rezistente la discreditare și demistificare, mai ales dacă aceste încercări sunt efectuate de către structuri identificate ca fiind oficiale, de stat (Sunstein, C.R. and Vermeule, A., 2009). Cu referire la teoriile conspirației, adesea se susține că oamenii, de fapt nu toți, dispun de puterea de a-și ascunde acțiunile, astfel că încercările de demistificare pot fi absorbite în povestea complotului și a conspirației.

Epoca în care trăim în prezent este foarte diferită de crizele epistemologice din trecut. Nu ne găsim într-o eră ideologică, în care să putem înlocui un adevăr cu altul, ci mai degrabă într-o perioadă a scepticismului sau a relativismului, unde se pune sub semnul întrebării însăși existența adevărului.

Noile tehnologii sociale și aplicații informatice facilitează schimbul rapid și pe scară largă de informații în cascadă, care pot răspândi dezinformarea, informațiile inexacte sau înșelătoare. În timp ce despre accesul nostru la informații și despre ghidarea știrilor de către aceste tehnologii știm câteva lucruri, nu știm prea multe despre contribuția lor exactă la caracteristicile procesului de răspândire a falsității și a adevărului în online. Sunt, de asemenea, cunoscute diferite modele teoretice de difuzare a zvonurilor sau metode pentru detectarea zvonurilor, de evaluare a credibilității informațiilor și, de asemenea, sunt cunoscute intervenții pentru reducerea răspândirii zvonurilor. Cu toate acestea, sunt puține studii robuste care să evalueze de ce știrile false se răspândesc altfel decât știrile adevărate. Rezultatele unui studiu elaborat de Soroush Vosoughi, Deb Roy și Sinan Aral (2018) au fost dramatice. Analiza rezultatelor înregistrate a relevat faptul că timpul de propagare al unei informații adevărate, la 1.500 de persoane, a fost de 6 ori mai mare decât timpul de propagare al unei informații false. Aceștia au demonstrat că știrile false din domeniul politic au fost mai virale decât oricare altă categorie de informații false. Știrile politice false, se arată în acest studiu, s-au propagat mai adânc în straturile societății de aproape trei ori mai repede decât toate celelalte

tipuri de știri false. Mai mult, o analiză a tuturor categoriilor de informații false a arătat că știrile din domeniul politic, dar și legendele urbane, s-au răspândit mult mai rapid decât știrile false din știință. De asemenea, s-a estimat că există șanse mai mari, cu o probabilitate de 70%, ca o știre falsă să se întoarcă la emițător decât o știre adevărată.

Ce ar putea explica astfel de rezultate surprinzătoare? După cum au observat și mulți alți cercetători, noutatea informației atrage atenția oricărui individ; de asemenea, gradul de contribuție la luarea unor decizii eficiente, precum și încurajarea schimbului de informații, despre care adesea se afirmă că poate actualiza înțelegerea noastră asupra lumii, concură la răspândirea rapidă a informațiilor.

Atunci când informațiile sunt noi, sunt nu numai surprinzătoare, ci sunt și valoroase, atât din perspectiva teoriei informației, întrucât oferă un ajutor mare pentru luarea deciziilor, cât și din punct de vedere social, deoarece transmit un mesaj important despre status-ul social al individului și anume că este unul „care știe” sau are acces la informații.

Includerea de roboți, în studiul vitezei de propagare a știrilor, nu a accelerat răspândirea știrilor false în detrimentul celor adevărate, efectul fiind aproximativ egal. Acest lucru sugerează că, opus a ceea ce mulți cred, știrile false se difuzează mai departe, mai rapid, mai adânc și mai larg în toate straturile sociale decât știrile adevărate deoarece oamenii, și nu roboții, sunt mai „eficienți” în propagarea acestora.

Care este răspunsul la întrebarea „ce conduce la răspândirea mai rapidă a știrilor false”? Se poate concluziona fără echivoc - comportamentul uman contribuie mai mult la răspândirea știrilor false decât inteligența artificială.

A existat o creștere a interesului cercetării privind modul în care oamenii răspund la corecțiile dezinformării, adică rectificarea informațiilor care sunt inițial presupuse a fi adevărate, dar mai târziu sunt dovedite a fi false (Schwarz, Newman și Leach, 2016).

Acești cercetători au ajuns la concluzia că, rareori, rectificările sunt pe deplin eficiente,

adică, în ciuda faptului că informația falsă a fost corectată și în ciuda recunoașterii validității corecției, oamenii continuă să se bazeze, cel puțin parțial, pe informațiile pe care le cunosc ca fiind false. Acest fenomen este cunoscut ca efectul influenței continue și a fost observat într-o gamă largă de studii (Ecker, Lewandowsky & Tang, 2010).

În anumite circumstanțe, și anume când rectificarea unei informații provoacă/afectează credințe larg acceptate de public, încrederea în informațiile false poate chiar să crească în mod ironic (Nyhan & Reifler, 2010). Au fost raportate constatări similare în studiile care au avut ca subiect mesajele cu privire la schimbările climatice (Hart & Nisbet, 2012) și vaccinările (Nyhan, Reifler, Richey și Freed, 2014).

Astfel, corecțiile unor informații sunt eficiente numai atunci când sunt îndeplinite cel puțin două condiții: în primul rând, ele nu trebuie să conteste în mod direct viziunea oamenilor asupra lumii. Acest lucru se poate realiza, de exemplu, afirmând valoarea de sine a publicului țintă care beneficiază de corecția informațiilor false sau făcând aprecieri convingătoare cu referire la mijloacele media care au transmis sau inițiat manipularea informațională (Nyhan & Reifler, 2010).

În al doilea rând, corecțiile trebuie să explice de ce dezinformarea a fost diseminată sau trebuie să se ofere o explicație robustă, logică, ca alternativă la evenimentele relevante. Pare tentant să concluzionăm că îmbunătățirea tehnicilor de comunicare și corecțiile mai eficiente ale informațiilor false pot fi suficiente pentru a pune capăt dezinformării pervazive.

Dar această concluzie ar fi prea simplistă. În schimb, susținem că rezolvarea efectelor manipulării informaționale necesită luarea în considerare a contextului politic, social și tehnologic mai larg, în care dezinformarea se desfășoară. Această comunitate epistemologică alternativă nu este ușor de perforat prin dovezile empirice sau corecțiile emise de mass-media sau de elite. Rezultă că înțelegerea originilor acestei lumi a post-adevărului necesită analiza mega-tendințelor politice și sociale, pe decade.

Unii autori au prezentat câteva tendințe societale care au contribuit la apariția post-adevărului în ultimele decenii (Lewandowsky, Ecker, Cook, 2010). Alegerea tendințelor s-a bazat pe probabilitatea existenței unei legături a acestora cu apariția unor mișcări politice mai radicale și extremiste, care, la rândul lor, este probabil să se bazeze mai mult pe ideologie decât pe dovezi.

Există dovezi despre scăderea pe termen lung a capitalului social, concept ce se referă la factori precum bunăvoința, empatia, încrederea între oameni și încrederea lor în instituțiile publice, precum și angajamentul lor civic (Aldrich & Meyer, 2015).

Într-o cercetare pe un eșantion numeros de respondenți (Twenge, Campbell și Freeman, 2012), s-a evidențiat că încrederea tinerilor din societatea occidentală în guverne a scăzut considerabil începând cu mijlocul anilor 1970.

Totodată, la nivelul populației din statele occidentale s-a observat o reducere semnificativă a numărului de confidenți, adică a oamenilor cu care aceștia pot să împărtășească o chestiune privată, fără teama de a le fi trădată încrederea. În timp ce în studiile din 1985 respondenții au evaluat că au în medie trei persoane considerate a fi confidenții lor, în 2004 numărul confidenților a scăzut la doi (McPherson, Smith-Lovin, & Brashears, 2009). În studiile care au repetat chestionarea acelorași aspecte ale capitalului social, din 2009, un sfert din respondenți au raportat că nu aveau niciun confident (Sander & Putnam, 2010) și aproape jumătate dintre respondenți au afirmat că au doar un confident, acestea fiind, în mod evident, aspecte caracteristice izolării sociale.

Dar, declinul capitalului social a fost însoțit și de schimbări ale valorilor sociale. Astfel, importanța faptului de a avea bani, prin contrast, s-a dublat, de la 40% în 1966 la aproximativ 80% în 2008 (Twenge et al., 2012), iar acest fenomen a fost însoțit de creșterea inegalității veniturilor cu toate consecințele derivate. Consecințele inegalității sunt multiple și au fost examinate temeinic, dar mai ales au fost analizate cele legate de polarizarea ideologică (Piketty & Saez, 2014; Wilkinson & Pickett, 2009).

Nicio analiză contemporană a tendințelor societății nu poate fi completă fără să comenteze transformarea rapidă a peisajului mediatic. Această transformare a fost analizată în detaliu în ultima decadă (Curran, Fenton, Freedman, 2012). În studiul acestora sunt prezente dovezi care dezvăluie legăturile dintre transformarea peisajului mediatic, polarizarea ideologică și apariția unei societăți fertile pentru dezvoltarea fenomenului numit „post-adevăr”.

În primul rând, flexibilitatea și fracționarea oferită de media au permis indivizilor să-și aleagă sursa „ecou” preferată, cu ale cărei informații disponibile, atitudini și prejudecăți preexistente rezonază cel mai mult.

O consecință a expunerii la partizanatul ideologic al mijloacelor media online a fost formarea unor credințe inexacte, chiar și atunci când erau dovezi relevante ce aveau menirea să corecteze acele credințe (Garrett, Weeks & Neo, 2016). Proliferarea mass-media online, combinată cu diferite platforme care livrează în mod obișnuit conținut consonant cu comportamentele utilizatorului, au accelerat rapid crearea de realități epistemice alternative (Del Vicario și colab., 2016).

De aceea, în opinia unor autori, creșterea consumului de știri este adesea asociată cu creșterea probabilității ca acești indivizi să fie dezinformați cu privire la diferite aspecte, cum ar fi existența unui consens științific puternic asupra schimbărilor climatice (Ramsay, Kull, Lewis & Subias, 2010), iar discursul ideologizat distribuit online a devenit caracterizat de agresivitate extremă, manipulare și fanatism.

Pot oamenii să devină mai rezistenți la încercarea de subminare a epistemologiei lor de către retorica de tip post-adevăr? Există cel puțin două considerente etice importante care trebuie să fie luate în considerare atunci când se caută răspunsuri la această întrebare legitimă.

În primul rând, chiar dacă s-a menționat în mod repetat legătura puternică între viziunea asupra lumii, pe de o parte, și susceptibilitatea la dezinformare și rezistența la corectarea sa, pe de altă parte, nu înseamnă că viziunile indivizilor despre lume ar trebui să fie schimbate.

Dimpotrivă, oamenii de știință trebuie să respecte și să protejeze credințele, opiniile politice și ideologiile personale (Lewandowsky, S., Ecker, U.K.H. & Cook, J., 2017).

În schimb, se susține că viziunea indivizilor asupra lumii ar trebui să fie decuplată de înclinația de a accepta dezinformarea și de a rezista corectării sale, de exemplu, prin căutarea unor mesageri care pot furniza indivizilor informații fără a-i provoca emoțional.

Este permisă și etică căutarea unor canale optime de comunicare pentru întreaga gamă, este drept foarte largă, de opinii personale, dar nu ar fi corect, din punct de vedere etic, să se dezvolte instrumente pentru a schimba viziunea oamenilor asupra lumii.

În al doilea rând, soluția recomandată, în general, împotriva dezinformării nu este implicarea directă, cenzura sau alte mijloace nedemocratice. Se susține crearea unei arhitecturi de informații de calitate, generată printr-un proces transparent, profesionist și democratic, favorabilă circulației informațiilor mai degrabă decât dezinformării.

În același timp, se susține și nevoia educării oamenilor, în sensul creșterii capacității de gândire critică. Sunt dovezi substanțiale care demonstrează că gândirea critică poate fi îmbunătățită printr-un program adecvat de instruire (Griffin and Mc Clary, 2015). Totuși, utilizarea strategiei post-adevăr poate să înceteze doar atunci când eficacitatea ei se reduce. Acest lucru poate apărea odată ce publicul reușește să recunoască obiectivele subiacente ale diferitelor politici și atunci când discrepanțele dintre propaganda ideologică și rezultatele reale ale acesteia vor deveni vizibile.

Concluzii

Toate acestea sunt o reflectare modestă a unei probleme în continuă creștere în lumea modernă și este absolut necesar să se înțeleagă clar de ce oamenii cedează diferitelor forme de dezinformare, care acum par să ne inunde zilnic. Într-un moment în care adevărul este împotmolit, este deosebit de important să înțelegem de ce credințele inexacte sunt reținute.

Drumul către educarea publicului cu privire la manipularea informațiilor, propagandă, dezinformare, fakenews, post-adevăr, este plin de opreliști și capcane. O capcană potențială este credința că doar prin îmbunătățirea comunicării sau prin generarea mai multor informații de calitate va fi suficient pentru a avansa. Există, în rândul comunității științifice, convingerea că acest lucru este insuficient - singură, comunicarea nu poate rezolva conflictele ideologice profunde, lupta pentru putere și împotriva democrațiilor. Rezultatele studiilor prezentate indică faptul că gândirea analitică joacă un rol important în protecția oamenilor împotriva dezinformării.

Acest lucru sugerează că intervențiile care au drept scop să facă publicul mai rezilient și mai atent la consumul de informații generează promisiuni realiste.

Bibliografie:

1. BRONNER, G  rald, *La D  mocratie des cr  dules*, PUF, 2013.
2. COHEN, G.L., ARONSON, J.; STEELE, C.M., „When beliefs yield to evidence: Reducing biased evaluation by affirming the self”, *Personality and Social Psychology Bulletin*, 2000, p.26.
3. CURRAN, J., FENTON, N., FREEDMAN, D., *Misunderstanding the Internet*, 2012.
4. THOMPSON, Damian, Counter-Knowledge: “How we surrendered to conspiracy theories, quack medicine, bogus science and fake history”, Atlantic, 2008.
5. DAVIS, J.J., *Advertising Research: Theory and Practice*, 2nd ed., Pearson, 2011.
6. Del VICARIO, M.; BASSI, A.; ZOLLLO, F., (2016). *The spreading of misinformation online*, National Academy of Sciences, p.113.
7. ECKER, U.K. H.; HOGAN, J.L., LEWANDOWSKY, S., “Reminders and repetition of misinformation: Helping or Hindering its Retraction”, *Journal of Applied Research in Memory and Cognition*, vol.6, Issue 2, p. 185-192, 2017.
8. ECKER, U.K.H.; LEWANDOWSKY, S.; TANG, D.T.W., “Explicit warnings reduce but do not eliminate the continued influence of misinformation”, *Memory and Cognition*, 38, 1087-1100, 2010.

9. ELLUL, Jacques, *Propaganda: The Formation of Men's Attitudes*, Vintage Books, 1973, pp.352.
10. MERCIER, H.; SPERBER, D., *The Enigma of Reason*, Harvard University Press, 2017, pp. 408.
11. GILOVICH, T., *How we know what so isn't: The fallibility of human reason in every day life*, New York: Free Press, 1991, pp. 224.
12. GREVE, W., & Wentura, D., "Immunizing the self: Self-concept stabilization through reality-adaptive self-definitions", *Personality and Social Psychology Bulletin*, 29, 2003.
13. GRIFFIN, M.; McClary, R., "A way to teach Critical Thinking", *Military Review*, 2015.
14. GUENTHER, C.L.; Alicke, M.D., "Deconstructing the better-than-average effect", *Journal of Personality and Social Psychology*, 99, 2010.
15. LEWANDOWSKY, S.; Ecker, U.K.H.; Cook, J., "Beyond Misinformation: Understanding and Coping with the Post-Truth Era", *Journal of Applied Research in Memory and Cognition*, 6:4, 2017.
16. LEWANDOWSKY, S., Ecker, U.K.H., and Cook, J., "Misinformation and the correction. Continued influence and successful debiasing", *Psychological Science in the Public Interest*, no. 3, vol. 13, 2012, p. 106-131.
17. NYHAN, B., Reifler, J., Richey și Freed, G., L. (2014), *Effective messages*, Pediatrics.133.
18. NYHAN, B., Reifler, J., When corrections fail, *Political Behavior*, 2010, 32(2), p. 303-330.
19. RAMSAY, C., Kull, S., Lewis, E., SUBIAS, S. (2010), *Misinformation*, University of Maryland.
20. HARDIN, Russell, "The Crippled Epistemology of Extremism", in A. Breton, G. Galeotti, P. Salmon & R. Wintrobe (eds.), *Political Extremism and Rationality*, Cambridge University Press, 2002.
21. SCHWARZ, N., NEWMAN, E., Leach, W. (2016). "Making the truth stick and the myths fade: Lesson from cognitive psychology", *Behavioral Science and Policy*, 2.
22. VOSOUGHI, Soroush, ROY Deb, ARAL Sinan: "The Spread of true and false news online", *Science*, 9 March 2018.
23. SUNSTEIN, C.R., Vermeule, A., "Conspiracy Theories: Causes and Cures? *The Journal of Political Philosophy*, 17:2, 2009.
24. TWENGE, J. M., Campbell, W. K., Freeman, E.C. (2012). "Generational differences in young adults life goals", *Journal of Personality and Social Psychology*, 102.

PROVOCĂRI ASOCIATE SURSELOR DESCHISE ÎN ACTIVITATEA DE INTELLIGENCE

*Rareș TĂBLEȚ**

Abstract

Taking into consideration the permanent changes regarding the structure, the content and the way of reaching the objectives by using the open sources of information, the need for quick adaptation of the intelligence agencies to the new realities is obvious. In a time characterized by constant and complex informational aggressions, executed by different strategic actors, the education of the target audience has a crucial role in achieving a high level of its resilience to hybrid actions.

Open sources remain a continuous challenge for intelligence agencies, both in terms of monitoring hostile entities and identifying authors/participants.

Keywords: open sources, OSINT, intelligence agencies, intelligence, hybrid warfare.

Motto: „Open sources can propagate to fill all the nooks and crannies that people want it to fill”.

Mitch KAPOR
fondator Lotus Software

Introducere

Lucrările de specialitate evidențiază tot mai des faptul că, în ultima perioadă, nicio structură de intelligence nu a mai putut ignora avertizările venite din zona surselor deschise de informații. O serie de acțiuni periculoase pentru siguranța și securitatea unui stat (terorism, îndoctrinare și radicalizare, propagandă, fake news etc.) își pot avea rădăcina în rețele de socializare, posturi de televiziune sau în diferite

site-uri, astfel încât nevoia de adaptare rapidă a structurilor de intelligence la noile realități este evidentă.

Ultimii ani au demonstrat că războiul hibrid l-a înlocuit cu succes pe cel convențional, tehnologia modernă având o pondere tot mai mare în ceea ce privește dotarea beligeranților. Instruirea continuă a personalului din domeniile OSINT și cyber, programele de educare



**Autorul este expert în cadrul Ministerului Apărării Naționale.*

a populației și colaborarea între structurile de informații reprezintă doar câteva dintre metodele prin care această provocare modernă poate fi controlată.

Reziliența la acțiunile informaționale

Un reper fundamental al societății actuale este viteza de diseminare a informațiilor și posibilitățile variate de a focaliza mesajul de interes asupra unui public țintă. În baza unor analize, deseori facile, referitoare la caracteristicile mediului social de interes, se pot identifica cele mai convenabile instrumente de atac informațional (din punct de vedere al rezultatului, efortului financiar sau resursei umane alocate).

Pe acest palier, provocarea pentru structurile de informații este de a identifica noile tehnici abordate și platformele de diseminare a mesajelor manipulatorii, pentru a putea oferi întregului aparat destinat comunicării strategice și resorturilor educaționale aflate la dispoziție posibilitatea contracarării oportune, în scopul diminuării efectelor.

O mare responsabilitate în atingerea acestui deziderat îi revine factorului educațional, care poate contribui fundamental la creșterea nivelului de cultură în domeniu și, implicit, a posibilităților de dezvoltare a gândirii critice a publicului țintă.

De la caz la caz, în funcție de obiectivul agresorului, dezvoltarea tehnologică actuală permite utilizarea unei varietăți mari de instrumente în scopul transmiterii mesajelor de interes: media clasică sau online, platforme de socializare, aplicații dedicate transmiterii informațiilor specifice zonei *gaming*, analize/lucrări de specialitate prezentate în cadrul unor conferințe/simpozioane etc.

Apreciem că structurile de informații au un rol important în răspunsul la aceste provocări variate, din punct de vedere al instrumentelor utilizate și abordărilor sau tehnicilor de manipulare aplicate, rol care se poate structura pe mai multe niveluri:

a. Identificarea

Experiența acumulată, nivelul ridicat de

cunoaștere și pregătirea continuă în domeniu permit unui specialist determinarea unor noi instrumente, vectori, modalități de acțiune sau obiective ale unui agresor informațional. Acest deziderat poate fi atins într-un mod facil și prin intermediul unei memorii instituționale complete și riguros augmentate. Este foarte importantă identificarea oportună a acțiunilor și a impactului acestora, mai ales în factorul *timp* (este o acțiune cu obiectiv pe termen scurt sau mediu), înainte ca acestea să pătrundă în mentalul colectiv țintă, pentru a facilita reacțiile în vederea contracarării.

b. Stabilirea publicului țintă și a scopurilor atacurilor

Analiza retoricii, a liniilor narrative din cadrul materialelor identificate permite, deseori cu exactitate, identificarea categoriei sociale avute în vedere, precum și obiectivele atacurilor.

Trebuie să reliefăm că, pentru a determina aceste aspecte, analistul de intelligence trebuie să dețină cunoștințe aprofundate referitoare la cultura, tradițiile, interesele, dar și reacțiile publicului țintă.

Bineînțeles, aceste elemente sunt vitale și celui care generează acțiunea informațională, motiv pentru care trebuie avută în vedere posibilitatea ca acesta să utilizeze și vectori interni.

c. Propuneri de contracarare

În principal, în funcție de concluziile analizelor efectuate, apreciem că modalitățile de contracarare pot avea în vedere, printre altele, utilizarea comunicatorilor oficiali (reacție rapidă) sau consolidarea eforturilor educaționale în vederea creșterii rezilienței. Dacă identificarea acțiunilor de tip informațional, a vectorilor și instrumentelor utilizate este, fără dubii, facilitată de existența unor aplicații dedicate acestui scop, interpretarea datelor obținute și stabilirea concluziilor nu se pot realiza decât de către specialiști cu un grad ridicat de cunoaștere și pregătire profesională.

d. Cultivarea gândirii critice

Unul dintre scopurile importante ale unei structuri de informații este combaterea

operațiunilor adverse, inclusiv prin prevenirea acestora. În domeniul acțiunilor informaționale, educația publicului țintă este unul dintre cele mai consistente mijloace de contracarare sau limitare a rezultatelor activității entităților ostile. În cadrul unei societăți care trăiește pe fundalul unei cantități uriașe de informații și interacționează constant cu aceasta, un deziderat al unei structuri care acționează pentru limitarea acțiunilor informaționale ostile este augmentarea capacităților propriului personal

Prezentăm o scurtă descriere a tehnicii:

Stop

- Nu distribuiți în mediul online materiale înaintea unei analize referitoare la conținut și veridicitate: *Think Before You Share*.

Investigate the source

- Efectuați întotdeauna o investigație primară și rapidă referitoare la sursa mesajului: analiza credibilității;
- Potrivit materialului, o verificare uzuală



în a identifica elementele de manipulare și dezinformare existente în spectrul public.

Potrivit unui material¹ recent publicat de LARICS², Mike Caulfield, directorul departamentului *Instruire combinativă și în rețea*³ din cadrul Washington State University, a elaborat o metodologie prin care publicul poate fi „educat” în vederea efectuării unor evaluări de bază pentru selectarea și verificarea informațiilor (fact-checking).

Denumit **SIFT**⁴, modelul a fost elaborat de expertul american în urma studiilor și observațiilor sale referitoare la lipsa abilităților și deprinderilor de bază ale studenților în verificarea informațiilor.

Metodologia⁵ cuprinde patru pași:

- *Stop*;
- *Investigate the source*;
- *Find better coverage*;
- *Trace claims, quotes and media to the original context*.

Conform autorului, SIFT solicită timp relativ scăzut destinat verificării unei surse și poate fi implementat de o persoană cu un nivel al cunoștințelor minim în operarea infrastructurii informaționale.

ar trebui să fie efectuată pe platforma Wikipedia, iar în cazul în care nu este identificată nicio pagină Wikipedia a respectivei surse, „cel mai probabil că avem de-a face cu un site din zona «ecosistemului mass-media marginale», creat special pentru a ne pune pe piste greșite”⁶.

Find better coverage

- Verificarea încrucișată a știrilor: căutare și stabilire dacă informația de interes a fost furnizată și de alte surse; uneori, în cazul acestei căutări, se pot obține inclusiv analize care demontează respectiva știre, publicate pe site-urile de fact-checking.
- Căutări după imagine: atunci când informația pivotează în jurul unei imagini asupra căreia planează incertitudinea originalității, se recomandă utilizarea funcției *reverse image search* pusă la dispoziție de Google.
- Motorul de căutare va afișa rapid o listă de surse care au folosit imagini similare cu cea de interes; în contextul în care constant imaginile sunt preluate de la alte

bellingcat

evenimente sau știri și refolosite, trebuie verificate data și sursa inițială.

Trace claims, quotes, and media to the original context

- Verificarea datei publicării: chiar și în cazul unei surse credibile, trebuie verificat contextul publicării materialului jurnalistic; există posibilitatea unui proces de redistribuire a unor știri, care pot conține informații depășite sau se pot încadra în *breakingnews fake*.
- Verificarea rapidă a conținutului: una dintre cele mai frecvente și dăunătoare tehnici de dezinformare este falsa recontextualizare – combinarea unor elemente și fapte reale cu unele false pentru reinterpretarea narațiunii /folosirea unor elemente și fapte reale, dar rezumând narațiunea într-o manieră manipulatorie.

Potrivit autorului analizei LARICS, „a cultiva o obișnuință zilnică în a verifica informația primită prin intermediul presei sau a social-media înseamnă un antrenament al gândirii critice și poate reprezenta una dintre soluțiile prin care ne putem feri de dezinformări”⁷.

Descoperirea acțiunilor adverse și a factorilor implicați

O altă provocare a structurilor de informații în domeniul surselor deschise este dată de deoalarea acțiunilor entităților ostile și identificarea autorilor/participanților. Existența unor capacități tehnologice, permanent actualizate, și gestionarea optimă a acestora creează circumstanțe favorabile unor succese remarcabile înregistrate de structurile de informații, în urma analizei datelor obținute din surse deschise.

Totodată, creșterea șanselor de contracarare a acțiunilor de tip hibrid este proporțională cu nivelul de cunoaștere/pregătire al resursei umane implicate: permanenta modificare a scopurilor, modalităților acționale și structurilor implicate sunt realități de care trebuie să țină cont o structură de informații performantă.

Un element argumentativ, în echilibrul capacități tehnice – resursă umană specializată, este oferit de analiza⁸ publicată pe portalul Bellingcat, la 14.08.2020, sub titlul „Putin Chef’s Kisses of Death: Russia’s Shadow Army’s State-Run Structure Exposed”⁹.

Bellingcat este o organizație independentă internațională, cu sediul la Amsterdam, formată din cercetători, investigatori și jurnaliști care elaborează analize fundamentate pe surse deschise de informații, inclusiv social media.

Potrivit prezentării¹⁰ de pe site-ul propriu, organizația are personal și colaboratori în peste 20 de țări, operează cu date publice, dispune de tehnologii avansate (ex.: recunoaștere facială și simularea îmbătrânirii) și utilizează metode de cercetare criminalistică.

Cu domenii de interes diverse (securitate, spionaj, terorism, crimă organizată etc.), anchetele jurnalistice elaborate de grupul de investigații respectă principiile transparenței



Valeri Prigojin (în dreapta)

Sursa: <https://www.opendemocracy.net/>

și responsabilității, iar analizele rezultate sunt preluate de agenții de presă recunoscute internațional.

Din recentul material Bellingcat, reținem două demonstrații, realizate cu elemente obținute din surse deschise: (1) confirmarea legăturilor oligarhului rus Evgheni Prigojin cu liderii de la Kremlin și (2) demonstrarea legăturilor dintre gruparea privată de securitate „Wagner” și structurile de forță ale Moscovei.

Una dintre persoanele acuzate constant de mass-media occidentale ca fiind implicată puternic în managementul acțiunilor de „trolling”, oligarhul rus Evgheni Prigojin, proprietar al unui lanț de restaurante de tip catering, a intrat în anturajul președintelui Putin în anul 2001. Prigojin conduce un grup media pro-Kremlin, numit Patriot, care își propune să contracareze presa anti-rusă care „nu ia aminte la lucrurile bune care se întâmplă în țară”¹¹. Grupul media reunește patru website-uri de știri din Sankt Petersburg: RIA FAN, Narodnye Novosti, Ekonomika Segodny și Politika Segodnya, despre care mass-media apreciază că, împreună, obțin o audiență mai mare decât a agenției de stat ruse TASS sau a canalului pro-Kremlin RT. În noiembrie 2018, agenția Bloomberg¹² evidențiază că firmele omului de afaceri rus sunt implicate în asigurarea securității sau organizarea de campanii politice în zece țări africane (Angola, Guineea, Guineea-Bissau, Republica Democratică Congo, Zimbabwe, Libia, Madagascar, Mozambic, Sudan și Republica Centrafricană). În schimbul serviciilor companiilor sale, Prigojin beneficiază de drepturi de exploatare minieră, precum și de facilități pentru desfășurarea afacerilor. Potrivit unor acuzații prezentate de publicația Novaia Gazeta¹³, în urma unei investigații proprii, Prigojin coordonează și un grup de asasini care se ocupă cu lichidarea unor activiști și bloggeri opozanți ai președintelui Putin. De asemenea, o serie de anchete jurnalistice l-au menționat ca fiind în legătură cu grupul de mercenari Wagner care a sprijinit regimul sirian, a luptat în estul Ucrainei și a promovat interesele F. Ruse în Libia și Africa subsahariană.

Potrivit recenteii investigații, derulată de Bellingcat, The Insider și Der Spiegel, dezinformarea, interferența politică și operațiunile militare ale lui Prigojin sunt strâns legate de Ministerul rus al Apărării și GRU.

Conform analizei, infrastructura privată a omului de afaceri rus, alături de cea a altor antreprenori dependenți de guvern, cum ar fi Kostantin Malofeev, este posibil a fi utilizată pentru operațiuni de spălare de bani pentru operații în afara F.Ruse.

Dar cum poate fi demonstrată legătura dintre Prigojin și elita politică a Moscovei? Cum se poate demonstra că această legătură nu este fundamentată numai pe activitățile de catering la Kremlin și pentru armata rusă – activități recunoscute a fi executate de firmele lui Prigojin?

Materialul Bellingcat prezintă argumente în acest sens, care cu greu pot fi dezmințite:

- Bellingcat a analizat înregistrările telefonice ale lui Prigojin pentru o perioadă de opt luni (în perioada 2013-2014), obținute din e-mailurile asistentului personal al afaceristului rus, sparte în 2015 de gruparea de hackeri Shaltai Boltay (F. Rusă);
- E-mailurile conțineau facturile telefonice ale companiei lui Prigojin - Concord Consulting & Management – și, în urma identificării numărului personal al omului de afaceri prin intermediul unei aplicații de căutare numere de telefon, a rezultat că Prigojin a luat legătura, prin sute de convorbiri telefonice, cu întreaga conducere a Biroului Administrației Prezidențiale, FSB-ului, Serviciului Federal de Protecție (FSO) și Ministerului Apărării rus.

În concluzie, Bellingcat apreciază că, deși companiile lui Prigojin erau furnizoare de catering la Kremlin și Ministerul Apărării rus, nu este plauzibil ca această relație profesională să fi generat o comunicare atât de frecventă și la un nivel atât de înalt. Drept consecință, potrivit analizei, implicarea afaceristului rus, alături de instituțiile de forță ale Moscovei, excede caracterul oficial.

În ceea ce privește negarea implicării Kremlinului în acțiunile „grupului Wagner”¹⁴, aceasta a devenit ușor de demontat după ce liderul grupului, Dmitri Utkin, a fost reperat în timpul unei transmisii video de la o recepție organizată la Kremlin, care a avut loc la 9 decembrie 2016.

După ce a negat inițial prezența lui Utkin, secretarul de presă al președintelui rus, Dmitri Peskov, a recunoscut, în cele din urmă, că acesta a participat la eveniment.

Ulterior, un cont VKontakte axat pe activitățile mercenarilor a publicat o fotografie în care președintele Putin este alături de patru ofițeri Wagner decorați. În urma acestei apariții publice neplanificate, Dmitri Utkin/„Wagner” nu a mai fost niciodată văzut sau auzit în public. În ciuda aparentei retrageri a lui Utkin din activitățile Wagner, numele său nu a rămas în afara atenției.

La câteva luni după publicarea fotografiei de la Kremlin, în noiembrie 2017, o persoană care purta exact numele lui Utkin a fost numită în funcția de CEO al companiei de catering a lui Evgheni Prigojin, Concord Management and Consulting.

Atunci când a fost abordat de mass-media ruse pentru a comenta legăturile presupuse ale lui Concord cu grupul Wagner, Prigojin a răspuns că „numirea lui Dmitri Utkin - care nu a mai ocupat niciodată vreo funcție în cadrul grupului nostru - este o decizie a managementului privat” și a spus că nu deține alte cunoștințe despre vreo companie militară privată.

Concluzii

În ultima perioadă, granița dintre *real* și *virtual* a devenit din ce în ce mai subțire, uneori chiar inexistentă, așa că pericolele actuale -

terorismul, propaganda, acțiunile de îndoctrinare și radicalizare, fenomenul *fake news* - sunt extrem de ușor de propagat în mediul online.

Platformele de socializare constituie mediul ideal pentru desfășurarea războiului hibrid, pe componenta informațională, cu eforturi financiare considerabil mai mici față de cel convențional. Implicarea actorilor statali și non-statali în acțiuni de manipulare și propagandă, cooptarea adeptilor de către mișcările de radicalizare, intoxicarea populației cu *fake news* sunt doar câteva exemple prin care grupurile țintă pot fi afectate, iar educația este cea mai sigură cale de apărare.

Acțiunile de tip hibrid sunt într-o permanentă schimbare, fapt care necesită, în vederea contracarării eficace, o continuă perfecționare a mijloacelor tehnice și umane ale structurilor de informații. Importanța acestor acțiuni este confirmată inclusiv de liderul militar al F.Ruse, gl. Valeri Gherasimov, care susținea, fără echivoc, că în societatea contemporană „mijloacele nemilitare (...) au depășit, ca eficiență, forța armelor”¹⁵.

Bibliografie

1. CAULFIELD, Mike, Sifting through the coronavirus pandemic.
2. GHERASIMOV, Valeri, VPK Magazine, nr. 8(476)/2013.
3. STROESCU, Mara, „Cum să eviți pandemia informațională cu ajutorul tehnicii SIFT”, analiză LARICS.
4. www.bellingcat.com.
5. www.bloomberg.com.
6. www.educase.edu.
7. www.infodemic.blog.
8. www.novayagazeta.ru.
9. www.vpk-news.ru.

¹ Mara Stroescu, *Cum să eviți pandemia informațională cu ajutorul tehnicii SIFT*, online la www.larics.ro/larics-edu-1-cum-sa-eviti-pandemia-informationala-cu-ajutorul-tehnicii-sift, accesat la data de 21.08.2020.

² **Laboratorul pentru Analiza Războiului Informațional și Comunicare Strategică** funcționează ca structură componentă a Institutului de Științe Politice și Relații Internaționale din cadrul Academiei Române. Potrivit propriei descrieri, **LARICS** are ca principal scop analiza/evaluarea evenimentelor interne și externe, a presei internaționale, cu referire specială la România și Republica Moldova, în contextul unor confruntări purtate în spațiul mediatic care au ajuns la dimensiunea unor războaie informatice.

³ *Blended and networked learning*, potrivit www.members.educase.edu/michael-caulfield, accesat la data de 24.08.2020.

⁴ Stop, Investigate the source, Find better coverage și Trace claims, quotes and media to the original context (Oprește-te, investighează sursa, găsește referințe mai bune, urmărește faptele din context).

⁵ Mike Caulfield, *Sifting through the coronavirus pandemic*, online la www.infodemic.blog, accesat la data de 21.08.2020.

⁶ Mara Stroescu, op.cit.

⁷ Ibidem.

⁸ <https://www.bellingcat.com/news/uk-and-europe/2020/08/14/pmc-structure-exposed/?s=09>, accesat la data de 24.08.2020.

⁹ *Sărutul morții din partea bucătarului lui Putin: armata din umbră a F. Ruse a fost expusă.*

¹⁰ <https://www.bellingcat.com/about/>, accesat la data de 24.08.2020.

¹¹ <https://www.bellingcat.com/news/uk-and-europe/2020/08/14/pmc-structure-exposed/?s=09>, accesat la data de 24.08.2020.

¹² <https://www.bloomberg.com/news/articles/2020-06-05/russians-sought-to-meddle-in-vote-libya-prosecutor-letter-shows>, accesat la data de 24.08.2020.

¹³ <https://novayagazeta.ru/articles/2018/11/08/78496-provokatsii-prigozhina>, accesat la data de 24.08.2020.

¹⁴ *Wagner* este o companie fondată de Dmitri Utkin, fost ofițer GRU, născut în 1970. Armata de mercenari a intrat în atenția publică în timpul conflictului din Ucraina/2014, în urma căruia F.Rusă a anexat Crimeea. Atunci a fost dezvăluit faptul că mercenari ai Grupului *Wagner* au luptat alături de forțele separatiste susținute de Kremlin.

¹⁵ Valeri Gherasimov, „Ценность науки в предвидении *Voенно-promyshlennyy Kuryer*”, online la www.vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf, pag. 2, accesat la 24.08.2020.

UTILIZAREA REȚELELOR SOCIALE. RISURI ȘI VULNERABILITĂȚI LA ADRESA PERSONALULUI MINISTERULUI APĂRĂRII NAȚIONALE

Răzvan ZMĂDU*

Abstract

The influence of robotics, artificial intelligence, 3D printing, and automation/standardization can be seen in both skilled and unskilled labor. The broad social and economic benefits of the products and services provided by modern technologies could be massive on short term and there might only be a few big winners and many more losers in the short term. Implications are huge: the biggest risk to all of the emerging technologies is the lack of Internet safety and security. Nowadays, the military organizations are already affected and the visible impact is just the beginning. In addition, through the weaponization of Internet and social media using multi-layered security infrastructure of troll factories and bots able to project the power of “alternative realities”, the “enemies” can effectively challenge the “ground truth” of competing societies in order to advance highly disruptive innovations.

Keywords: social network, cyber security, cybercrime, social engineering, information warfare, network war, army, militaries.

Rețele sociale – istoric, definiție și concept

În cadrul evoluției și interacțiunii digitale de astăzi, rețelele sociale reprezintă cel mai utilizat produs al acesteia.

Definirea rețelelor sociale (*Social Media*) depinde de punctul de vedere al celui care analizează acest fenomen.

Pentru început, prin rețea socială „se înțelege deseori și o rețea [informațională] de utilizatori Internet, bazată pe anumite site-uri web la care utilizatorii se pot înscrie și interacționa cu alți utilizatori, deja înscriși”¹.

Pe de altă parte, o rețea socială „este un set de tehnologii și canale de comunicare care sunt folosite pentru a facilita crearea unei comunități uriașe și a permite membrilor ei

colaborarea productivă. Cele șase concepte care definesc rețelele sociale sunt: participativ, colectiv, transparent, independent, persistent și emergent. Aceste caracteristici combinate diferențiază social media de celelalte forme de comunicare”².

Dintr-o perspectivă ce se dorește mai cuprinzătoare, rețelele sociale reprezintă un grup de aplicații ce utilizează rețeaua Internet, constituite ideologic și tehnologic pe conceptul relativ nou, global, numit *Web 2.0*, care permite generarea și schimbul de conținut de către utilizatori.

Mișcarea de socializare a luat o amploare deosebită prin mutarea în mediul *online*, revoluționând societatea și modul de viață.

*Expert în Ministerul Apărării Naționale

Classmates.com	1995	
	1996	
Six Degrees.com	1997	
	1998	
LiveJournal BlackPlanet	1999	Asian Avenue
LunarStorm	2000	MiGente
Cyworld	2001	Ryze
Fotolog Skyblog	2002	Friendster
MySpace LastFM Hi5 Plaxo	2003	LinkedIn OpenBC/Xing Tribe.net SecondLife
Catster Care2 Hyves aSmallWorld Orkut Dig Flickr	2004	Facebook Piczo Mixi Dodgeball Multiply Dogster BiggerPockets
Ning Cyworld (China) Yahoo! 360	2005	YouTube Xanga Bebo Reddit
MyChurch Cyworld Stylehive	2006	Twitter QQ Fabulously40
Osmosus GlobalGrind	2007	Tumblr

Fig. nr. 1 Evoluția rețelelor sociale 1995-2006

Trebuie amintit mai întâi că *SixDegrees.com* este site-ul primei rețele sociale și a fost lansat în anul 1997. Acesta permitea utilizatorilor să își creeze un cont, să își listeze prietenii și din anul 1998 utilizatorii puteau vizualiza liste de prieteni. *SixDegrees.com* se remarcă prin aceste facilități, spre deosebire de un site asemănător, *classmates.com*, care permitea utilizatorilor doar afilierea la instituția de învățământ finalizată, fără posibilitatea de a crea un cont.

În continuare, între anii 1997 - 2001, au apărut mai multe rețele sociale, care înglobau comunități de utilizatori, pe baza anumitor criterii personale sau profesionale. Rețele precum *AsianAvenue*, *BlackPlanet*, *MiGente*, *Cyword*, *LunarStorm* au fost lansate în diferite colțuri ale mapamondului.

Începând cu anul 2001, constatăm un nou trend în cadrul rețelelor sociale, odată cu lansarea *Ryze.com*, prima rețea socială unde utilizatorii proveneau din mediul de afaceri din San Francisco.

Trendul a fost urmat în 2002 de *Friendster*, o rețea socială construită pentru a concura cu un site profitabil de întâlniri online, *Match.com*. Toate site-urile de întâlniri *online* de până atunci aveau ca principală caracteristică stabilirea de legături cu persoane necunoscute, pe când *Friendster* a fost conceput pentru a ajuta prietenii-prietenilor să se întâlnească, având ca argument faptul că întâlnirea cu cineva „cunoscut” este mai „sigură și avantajoasă” decât cu un necunoscut.

În contrast cu anii anteriori, anul 2003 este anul lansării mai multor rețele sociale cu un impact major în rândul utilizatorilor, *Xing* (inițial *openBNC*), *LastFM*, *Hi5*, *LinkedIn*, *MySpace*, *SecondLife* și *Tribe.net*.

Nu în ultimul rând, 2004 rămâne în istorie ca anul când cea mai populară rețea socială se lansează și anume *The Facebook*, denumirea inițială a rețelei. Începută ca o rețea în cadrul universității din Harvard, *Facebook* a căpătat

o amploare deosebită și în alte universități din Statele Unite ale Americii, precum Columbia, Stanford și Yale, ajungând la 1 milion de utilizatori pe 30 decembrie 2004. Rețeaua a ajuns la cifra de 1 miliard de utilizatori în octombrie 2012. În anul 2012, a achiziționat serviciul online de *photo-sharing*, *video-sharing* și rețea socială, *Instagram*, iar în anul 2014 aplicația de mesagerie gratuită, *WhatsApp*.

Cea mai nouă rețea socială apărută cu un impact major în rândul utilizatorilor este *Gabo*, fiind inspirată de *Facebook*. Rețeaua socială a apărut în iulie 2019, în Vietnam, succesul ei datorându-se și faptului că regimul comunist controlează mass-media locală.

Având în vedere aceste evoluții, se preconizează o amploare deosebită a rețelelor sociale, prin simplu fapt că numărul utilizatorilor de Internet va crește considerabil. Aceasta se datorează inclusiv implementării tehnologiei 5G în cadrul rețelelor de telefonie mobilă.

Uniunea Europeană, dar este sub rata țărilor din America de Nord și Asia de Sud-Est.

Rețeaua *Facebook* domină piața rețelelor sociale din România, cu aproximativ 10 milioane de utilizatori, la o distanță de peste 6 milioane de utilizatori față de următoarea rețea, *Instagram*, o subsidiară a platformei *Facebook*.

De asemenea, în țara noastră, rețeaua socială creată de Mark Zuckerberg este pe primul loc în ceea ce privește topul căutărilor după cuvinte cheie pe cel mai puternic motor de căutare Google Search, *google.ro*.

În consecință, cu un grad de utilizare zilnică a Internetului de 85%, românii sunt printre cei mai mari consumatori de conținut de pe rețelele sociale din Europa. Aceasta se datorează și faptului că țara noastră a ocupat, în anul 2018, locul 5 în lume la broadband, cu o viteză de descărcare de peste 91Mbps și de încărcare de peste 67 Mbps.

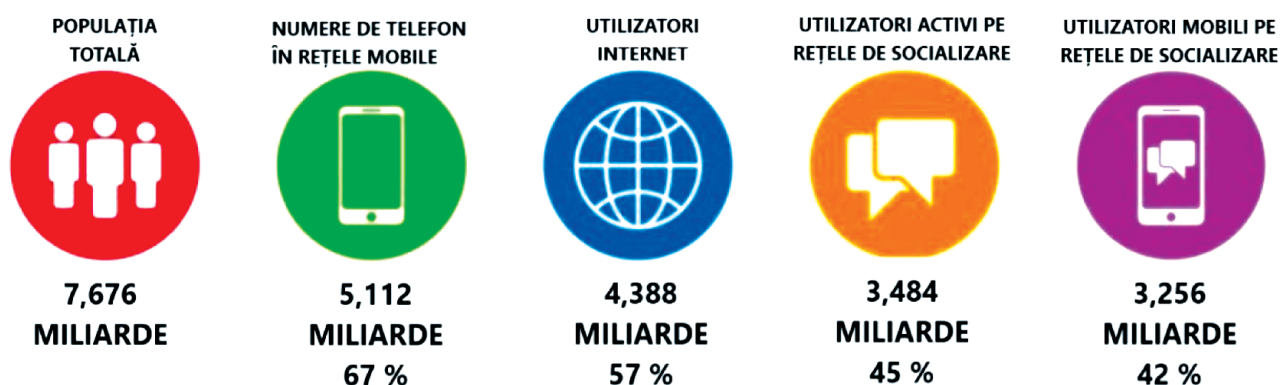


Fig. nr. 2 Numărul de utilizatori de Internet și rețele sociale raportat la populația globală

În anul 2019, la nivel mondial, 57% din populația totală de aproximativ 7,6 miliarde avea acces la rețeaua Internet. Gradul de utilizare a rețelelor sociale era de 45%, cu un nivel mai ridicat în America de Nord și estul Asiei.

În România, la o populație raportată la începutul anului 2019 de aproximativ 19 milioane de cetățeni, un procent de 77% are acces la rețeaua Internet. Dintre aceștia, 11 milioane (sau 56% din totalul populației) sunt utilizatori activi în cadrul diferitelor rețele sociale. Țara noastră se încadrează în cifrele țărilor din Europa și

Particularități ale utilizării de către personalul militar a rețelelor sociale

Avantajele rețelelor sociale sunt multiple, având în vedere numărul mare de utilizatori înregistrați. Fie că vorbim de știri din toate domeniile sau folosirea nelimitată a clipurilor video, rețelele sociale oferă un mod de comunicare *online*, prin email sau chat, dar și prin intermediul *microblogging*-ului³.

Rețelele sociale au devenit instrumente ale marketingului modern, prin care sunt prezentate valorile Armatei în cadrul comunităților în care

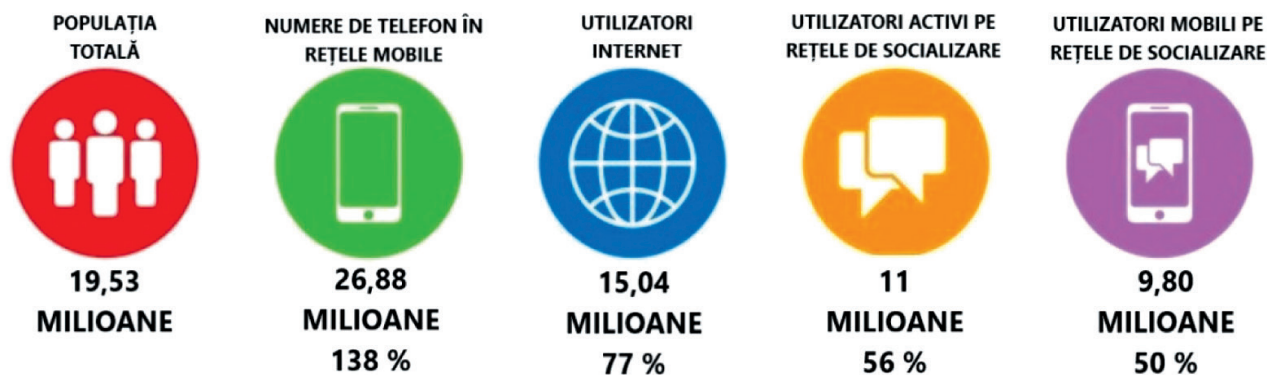


Fig. nr. 3 Numărul de utilizatori de Internet și rețele sociale raportat la populația României

militarii trăiesc și muncesc. Astfel, în cadrul Ministerului Apărării Naționale, în sistemul de apărare și securitate națională, dar și în structurile specializate, comandanții și șefi de la nivelurile tactic, operativ și strategic, utilizează rețelele sociale pentru comunicare, recrutare, suportul familiilor militarilor, desfășurarea de exerciții și antrenamente naționale și internaționale, misiuni ale militarilor în teatrele de operații, prezentarea performanțelor obținute de anumite structuri sau membri ai forțelor armate.

Prin urmare, la expansiunea comunităților de utilizatori ai rețelelor sociale s-a alăturat și personalul din cadrul sistemului de apărare și securitate națională, datorită creșterii nevoii acestuia de dezvoltare, informare și învățare, de comunicare online personală sau instituțională.

Schimbările provocate de rețelele sociale în societatea modernă au adus și anumite riscuri și vulnerabilități. Au existat situații când accesul la rețelele sociale a fost interzis complet. Astfel, în anul 2007, guvernul canadian a restricționat accesul angajaților la rețeaua socială *Facebook*, iar Armata Statelor Unite a interzis, în același an, militarilor accesul la rețeaua socială *MySpace*.

De asemenea, președintele Rusiei, Vladimir Putin, a declarat, pe 20 februarie 2019, că Rusia ar putea renunța la Internetul global datorită „imprevizibilității partenerilor noștri”. La o săptămână, purtătorul de cuvânt al Kremlinului, Dmitri Peskov, a precizat într-un interviu acordat presei ruse că „(...) date fiind aceste potențiale amenințări, se fac demersuri pentru adoptarea unei legislații, cum ar fi așa-numitul proiect de lege privind Internetul suveran”. Duma de Stat a adoptat legea „privind măsurile organizatorice, administrative și tehnice pentru protejarea Internetului în Rusia” pe 11 aprilie 2019, iar, printre altele, textul prevede deconectarea și funcționarea RuNet⁴ fără servere străine în cazul unor atacuri cibernetice, controlul și monitorizarea asupra întregului trafic de Internet din Rusia de către autorități. Legea a fost promulgată de Vladimir Putin pe 1 mai 2019 și a intrat în vigoare în luna noiembrie, iar prevederile referitoare la apărarea criptografică a informațiilor și sistemul național al numelor domeniilor se vor aplica de la 1 ianuarie 2021. Echipamentele care permit izolarea Internetului din Rusia de rețeaua mondială au început să fie

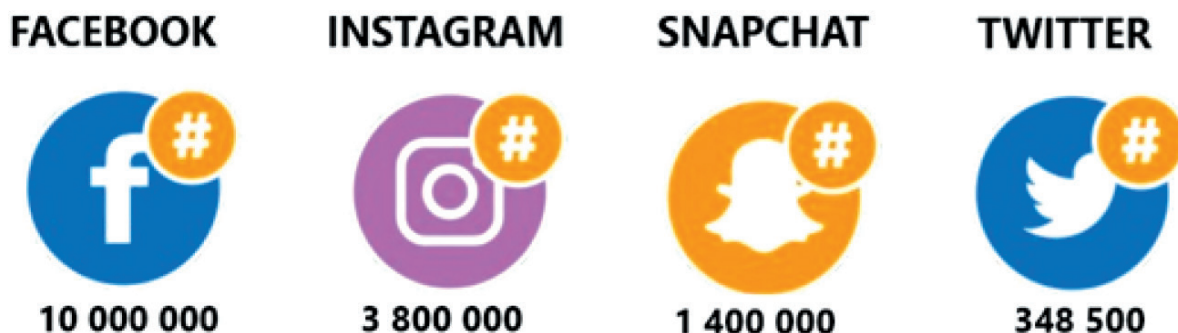


Fig. nr. 4 Topul rețelelor sociale din România

instalate începând cu luna septembrie 2019 de către Serviciul federal rus pentru supravegherea comunicațiilor, tehnologiei informației și mass-media, *Roskomnadzor*.

Trebuie avut în vedere faptul că, prin Hotărârea nr. 4546 din data de 27.11.2014, Înalta Curte de Casație și Justiție a decis în mod irevocabil că pagina de *Facebook* a fiecărui utilizator reprezintă un spațiu public și nu unul privat.

Prin urmare, expunerea publică a unor opinii proprii, găzduirea opiniilor altor persoane sau preluarea unor materiale din mediul virtual pe contul personal de pe Facebook ori pe contul altor persoane, sub un nume real sau fictiv, poate fi considerată ca o exprimare publică.

În consecință, postările militarilor pe rețeaua socială Facebook, dar și în alte aplicații considerate spațiu public, vor fi catalogate ca o exprimare în public și se vor supune unor reglementări specifice din domeniul informării și relațiilor publice. Militarii pot răspunde individual, aceștia având obligația de a respecta legile și normele conforme cu statutul profesional.

Riscuri și vulnerabilități la adresa personalului Ministerului Apărării Naționale

Nu mai este nicio îndoială că, până la acest moment, nu există rețea socială care să nu fie vulnerabilă, prezentând erori de conectare, scripturi „cross-site” sau java, pe care criminalii cibernetici le pot folosi sau exploata. Spre exemplu, în februarie 2010, un script a descărcat 215 milioane de profile de pagini ale rețelei sociale *Facebook*, printre care 120 de milioane de profile de utilizatori din Statele Unite ale Americii. Șase luni mai târziu, un consultant în securitate a scris un script care a descărcat datele a 171 milioane de utilizatori de pe *Facebook*.

De asemenea, în luna septembrie 2019, o bază de date ce conținea informațiile (nume utilizator, număr de telefon, genul și țara de origine) a peste 419 milioane de utilizatori *Facebook* a fost descoperită de specialiști în domeniul securității digitale.

Atunci când se constată că unii militari petrec prea mult timp pe rețelele sociale și mai

puțin în cadrul activităților curente, rețelele sociale pot fi percepute de către comandanți, șefi, ca o amenințare la adresa performanțelor și profesionalismului organizației militare, precum și a securității și siguranței operațiilor (OPSEC⁵).

Pe lângă probleme la locul de muncă, petrecerea îndelungată pe rețelele sociale conduce, de cele mai multe ori, la dependență. Utilizatorii rețelelor sociale devin captivi de fluxul de informații apărute, petrecând foarte mult timp în mediul online. Timpul îndelungat petrecut online poate genera pentru utilizator și probleme de integrare socială, dar și depresie. În acest sens, Universitatea din Harvard a publicat un studiu în care era demonstrat faptul că petrecerea îndelungată a timpului pe rețelele sociale poate conduce la o anumită formă de depresie. În comunitatea medicală se vorbește din ce în ce mai mult de *social media depression*, o stare produsă de nemulțumirile apărute din cauza unor utilizatori care își etalează succesul și opulența pe rețelele sociale. Modificările psiho-comportamentale sunt incompatibile cu calitatea de militar, iar acest tip de depresie poate fi speculat pentru manipularea unui grup țintă în scopul destabilizării acestuia și inducerea unui sentiment de nemulțumire față de instituțiile statului, în cazul de față Ministerul Apărării Naționale, care devine, astfel, responsabil pentru nivelul scăzut de trai.

În cadrul Ministerului Apărării Naționale și în tot sistemul de apărare și securitate națională sunt vehiculate informații clasificate, cu respectarea prevederilor Legii nr. 182 din 04 decembrie 2002 privind protecția informațiilor clasificate. Divulgarea unor informații militare reprezintă o vulnerabilitate tot mai prezentă pe rețelele sociale. Acestea încurajează utilizatorii să posteze imagini, filme și comentarii despre activitățile desfășurate, locuri vizitate, impresii, calificative. Prin anumite postări pot fi divulgate informații care nu sunt destinate informării publice, dar pot fi și încălcate anumite reguli privind informarea și relațiile publice în Ministerul Apărării Naționale.

În același timp, statutul cadrelor militare prevede că „prezentarea, în public, de informații

cu caracter militar de către cadrele militare nu este permisă, cu excepția celor care au atribuții în acest sens, potrivit normelor stabilite prin ordin al ministrului apărării naționale”⁶.

În această privință, cea mai recentă dezvăluire a unor informații sensibile este despre exercițiul *Trident Juncture 2018*, cea mai mare demonstrație de forță din ultimii 30 de ani a NATO. Astfel, ziarul *New York Times* publică, în ediția din 21 februarie 2019, un articol care dezvăluia că mișcărilor de trupe, nave și operațiile exercițiului au putut fi monitorizate pe rețelele sociale prin simpla urmărire a hashtag-ului⁷ *#Tridentjuncture*.

Disciplina militară este o caracteristică importantă a forțelor armate, numai că încălcarea ei s-a mutat în mediul online. Tot mai mulți utilizatori adaugă conținut sau comentarii negative despre Armată și conducătorii ei de la diverse eșaloane, fapte care compromit onoarea și demnitatea militară.

Așadar, prin Legea nr. 80 din 11 iulie 1995 privind statutul cadrelor militare, „cadrelor militare în activitate le este restrânsă exercitarea unor drepturi și libertăți”⁸, printre care și „exprimarea în public a unor opinii contrare intereselor României și forțelor armate”⁹.

Pe de altă parte, militarii răspund în cazul nerespectării actelor normative referitoare la interzicerea organizațiilor, simbolurilor și faptelor cu caracter fascist, rasist sau xenofob și a promovării cultului persoanelor vinovate de săvârșirea unor infracțiuni contra păcii și omenirii. Astfel, prin Legea nr. 217 din 23 iulie 2015, pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 31 din 13 martie 2002 privind interzicerea organizațiilor și simbolurilor cu caracter fascist, rasist sau xenofob și a promovării cultului persoanelor vinovate de săvârșirea unor infracțiuni contra păcii și omenirii, este precizat că săvârșirea unor fapte de promovare în public a unor astfel de organizații, simboluri și fapte, inclusiv „prin intermediul unui sistem informatic, constituie infracțiune care se pedepsește cu închisoare”.

De asemenea, „amenințarea unei persoane sau a unui grup de persoane, prin intermediul

unui sistem informatic, cu săvârșirea unei infracțiuni pentru care maximul pedepsei prevăzute de lege este închisoarea de cel puțin 5 ani, pe motiv de rasă, culoare, ascendență sau origine națională ori etnică sau în considerarea religiei, dacă aceasta este folosită ca pretext pentru oricare dintre motivele arătate, constituie infracțiune și se pedepsește cu închisoare de la un an la 3 ani”¹⁰.

Având în vedere că rețelele sociale au devenit mecanisme în lupta politică, utilizatorii cu drept de vot și-au manifestat apartenența politică. În schimb, conform Legii nr. 101 din 8 mai 2019 pentru modificarea și completarea Legii nr. 80/1995 privind statutul cadrelor militare, cadrelor militare în activitate nu le este permisă „exprimarea în public a opiniilor politice”¹¹.

Un alt pericol tot mai des întâlnit în zilele noastre este apariția de știri și informații ce utilizează instrumente specifice tehnicilor de dezinformare și propagandă sau care nu au declarate sursa sau furnizorul de servicii pe rețelele sociale. Putem vorbi despre *fake news*, fenomen ce datează din secolul XIII î.Hr. și care, prin manipularea opiniei publice, duce la dezechilibre sociale cauzate de scăderea nivelului de încredere al celor vizați. Tehnicile de manipulare au evoluat semnificativ, de la distribuția de manifeste din aeronave la utilizarea rețelelor sociale și a Internetului. Militarii trebuie să fie în măsură să filtreze astfel de informații false, prin verificarea fluxului de știri, dar și urmărirea unor platforme mass-media credibile. Recent, au apărut și în România soluții tehnice de verificare automată a faptelor din texte sau site-uri web care se ocupă cu *fact checking-ul*. Prin astfel de metode sunt evaluate și verificate veridicitatea unor știri apărute în mediul online.

Cu toate aceste metode de luptă împotriva fenomenului știrilor false, sunt cazuri când oamenii pun la îndoială o știre adevărată doar pentru că aceasta se află în contradicție cu opiniile și ideile personale.

Pe rețelele sociale pot apărea și situații periculoase pentru militari, deoarece acestea sunt



Fig. nr. 5. Militari din Forțele Speciale Române în teatrul de operații (sursa: Facebook)

folosite ca și canale de comunicații și propagandă pentru teroriști. Grupările extremiste sunt foarte active în mediul on line, unde recrutează adepți și își fac cunoscut manifestul.

Fără îndoială că cea mai mare amenințare la adresa militarilor rămâne crearea unei baze de date cu personalul din cadrul Ministerului Apărării Naționale de către grupări teroriste, servicii de informații externe sau grupări de crimă organizată. Acestea pot fi exploatare cu intenții ostile la adresa securității naționale, prin atacuri cibernetice sau non-cibernetice.

Riscul este cu atât mai mare, deoarece rețeaua *Facebook* oferă utilizatorilor posibilitatea de a indica o persoană dintr-o fotografie de grup, de a posta mesaje prin anumite instrumente care fac legătura dintre fizionomie și nume. Astfel, utilizatorii care nu au publicat datele personale pe rețea, pot fi identificați prin intermediul acestor mecanisme, fără acordul lor, ca urmare a activității unor prieteni.

Trebuie menționat și faptul că orice informație introdusă de către utilizatori pe rețele sociale rămâne stocată permanent, chiar dacă aceasta este ulterior ștearsă, indiferent dacă informațiile sunt greșite sau irelevante.

Drept dovadă, în cazul rețelei *Facebook*, ștergerea contului de utilizator nu duce la ștergerea definitivă a informațiilor și fotografiilor din cadrul acestuia. Acestea sunt stocate permanent pe serverele rețelei sociale, fiind disponibile și după moartea fizică a utilizatorului.

În plus, *Twitter*, considerată rețeaua socială nr. 2 în lume, a vândut drepturile de a interoga mesajele postate de utilizatori către companiile *Google* și *Microsoft*. Acestea au fost posibile deoarece termenii și condițiile de utilizare și politica de confidențialitate acordă exclusivitate asupra tuturor informațiilor și imaginilor postate.

Un alt fenomen tot mai întâlnit pe rețelele sociale este furtul de identitate. Dacă la începutul secolului al XIX-lea victimele erau ucise pentru a li se asuma identitatea, în prezent este utilizată tehnologia pentru a avea acces la informații personale care să fie asumate în cadrul furtului de identitate. Scopul acestuia este de a utiliza resursele persoanei sau de a obține anumite beneficii în numele acesteia.

În directiva 95/46/CE a Parlamentului European și a Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date sunt definite datele cu caracter personal ca fiind „orice informație referitoare la o persoană fizică identificată sau identificabilă; o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale”.

Astfel, „prezentarea sub o identitate falsă ori atribuirea unei asemenea identități altei persoane, pentru a induce sau a menține în

eroare un organ sau o instituție de stat sau altă unitate”¹² este sancționată de legislația națională în vigoare, prin Codul Penal.

Prin urmare, în aflarea de date personale ale utilizatorilor, sunt folosite o serie de tactici și tehnici specifice războiului cibernetic. Vorbim de inginerie socială (*social engineering*), pe care unii specialiști în domeniul securității cibernetică o numesc și *human hacking*. Astfel, criminalii ciberneticii folosesc următoarele metode:

- *Phishing* și *spear phishing* - tehnici de înșelăciune prin care se obțin date confidențiale și personale. Divulgarea acestora este determinată de un pretext foarte bine pus la punct de criminalii ciberneticii, aceștia clonând paginile de înregistrare/logare ale rețelelor sociale sau prin serviciile de chat ale acestora. *Spear phishing*-ul este un atac doar asupra unui individ anume sau asupra unei organizații; riscul și varietatea unor atacuri de acest tip va crește, deoarece actorii vor utiliza inteligența artificială pentru traducerea automată a mesajelor în toate limbile; Experții *Bitdefender* împreună cu specialiști ai serviciilor de informații naționale și internaționale au studiat și publicat un raport intitulat „ATP28, o călătorie în sustragerea de informații guvernamentale”¹³. Prin *spear phishing* au fost ținute figuri politice proeminente, instituții guvernamentale, servicii de telecomunicații și criminalitate informatică și companii aerospațiale din România, Germania și Ucraina.
- *Scam* – presupune inducerea în eroare a utilizatorilor, prin anumite postări care sunt accesate. Compania *Bitdefender* a realizat un top al acestor escrocherii, iar cea mai accesată în România a fost „vezi cine ți-a vizualizat profilul”, „verifică dacă te-a șters un prieten” sau „am aflat cum să îi văd pe cei care se uită la profilul meu”. În spatele acestor postări stau fișiere executabile care sunt rulate pe calculatoare sau dispozitive mobile și permit controlul asupra acestora.

Destinația acestor escrocherii au fost în special rețelele sociale *Facebook* și *Pinterest*.

- *Atac de tip watering hole*: este un tip de inginerie socială care se bazează pe încrederea utilizatorilor în anumite acțiuni desfășurate pe o pagină de Internet pe care o frecventează. Atacatorul pregătește un atac astfel încât utilizatorul nu va ezita să acceseze anumite link-uri către pagini cunoscute, dar care oferă acces la informații personale. Acest tip de atac a avut succes și în cazul unor sisteme informatice foarte bine securizate.
- *Baiting*, similar cu *phishing*, oferă un anumit avantaj în schimbul unor informații personale. „Momeala” poate avea diferite forme digitale (melodie, film care poate fi descărcat) sau fizice (un dispozitiv amovibil cu însemnele instituției). După descărcare, softul malițios este rulat automat și oferă atacatorului acces la tot sistemul informatic.
- *Quid pro Quo*: implică un schimb între utilizator și atacator. Atacatorul va solicita informații personale (email, adresă etc.) în schimbul unor servicii sau al unei sume de bani (ex.: participarea la un sondaj care oferă după completare o sumă de bani).
- *Piggybacking*: numit în literatura de specialitate și *tailgating*; cea mai întâlnită situație este atunci când atacatorul își solicită accesul la sistemul informatic personal sau de serviciu pentru o acțiune care nu trezește suspiciuni. Odată facilitat accesul, este introdus un soft malițios care oferă acces la informații critice.
- *Pretexting*: este atunci când atacatorul își creează o falsă identitate pentru a avea acces la informații sensibile. Este denumit și *phishing uman*.

Pentru identificarea militarilor pot fi folosite și alte instrumente sau tehnici permise de rețelele sociale. De exemplu, un consultant de securitate al Armatei americane a creat pe *Facebook* un cont fictiv al unei angajate de 25 de ani a *US Navy Network Warfare Command*.

În mai puțin de o lună, contul a strâns peste 300 de contacte din comunitatea de apărare și securitate din Armata americană, fiind invitată, printre altele, pentru a lua cuvântul la o conferință pe probleme de securitate și pentru a consulta documente tehnice emise de NASA.

Punerea la dispoziție a informațiilor referitoare la apartenența la un sistem național de apărare poate reprezenta un atu pentru entitățile specializate în culegerea de informații. În presa de specialitate au apărut articole unde erau prezentate cazuri de racolări ale militarilor de către femei, pe rețelele sociale. Cel mai recent caz a fost semnalat de departamentul de contraspionaj al Serviciului de Securitate al Ucrainei, care a detectat mai multe încercări de racolare a unor militari ucraineni de către FSB, (Serviciul Federal de Securitate al Federației Ruse).

Riscul de infectare a rețelelor militare cu *malware* și viruși prin rețelele sociale este real deoarece, pentru executarea de atacuri cibernetice, este folosită inclusiv inteligența artificială. Aceasta rescrie codul *malware* în funcție de lecțiile învățate din tentativele nereușite de atac.

Concluzii

Rețelele sociale constituie un factor pozitiv al vieții sociale, dar trebuie avută în vedere menținerea unui echilibru între virtual și viața reală. Dezvoltarea continuă implică și noi moduri de evaluare a acestora, dar și a modului de abordare a vieții sociale, economice, educaționale și politice de către comunitatea de utilizatori.

Prin urmare, sistemul militar evoluează și se transformă odată cu societatea modernă. Era informațională în care trăim a revoluționat conducerea acțiunilor militare și spațiile de luptă. Astfel, în strategiile de apărare și la nivel doctrinar, anumite state au introdus termeni precum spațiu de luptă virtual, război cibernetic sau război informațional, iar orice atac desfășurat este tratat ca o agresiune teroristă.

Tehnologia din domeniul comunicațiilor și informaticii a fost integrată în conducerea

acțiunilor militare, generându-se astfel sisteme performante de C4ISR¹⁴, capabile să asigure superioritatea în mediul operațional.

Astfel, rețelele militare au ajuns să fie o țintă tot mai valoroasă în spațiul de luptă virtual. Infractorii cibernetici folosesc metode și tehnici avansate, nedetectabile și greu de neutralizat, având ca scop accesarea de informații clasificate sau confidențiale din diferite sectoare ale armatelor naționale.

În cadrul războiului informațional, utilizarea rețelelor sociale reprezintă un pericol real pentru personalul din cadrul Ministerului Apărării Naționale, care poate răspunde penal, civil, material, disciplinar, social sau personal.

În paralel, noile dezvoltări tehnologice aduc în spațiul public (online sau offline) provocări de natură securitară, mai ales din perspectiva protecției la intruziunea tehnologiilor disruptive. Cele mai periculoase sunt cele duale (uz civil și militar), promovate atent, care sunt prezentate cu certe avantaje (interconectare, viteză, acces la servicii diverse, calitate etc.), dar care prezintă și dezavantaje/riscuri – mai puțin sau deloc conștientizate de oameni, fie ei și militari și lucrători din sistemul de apărare și securitate (vezi breșele de securitate tocmai din cadrul serviciilor de informații).

Principalele provocări de securitate ce derivă din dezvoltarea tehnologiilor disruptive, riscurile și vulnerabilitățile sistemice datorate, de cele mai multe ori, erorii umane, aduc în atenție necesitatea permanentă de securizare a utilizatorilor și adaptarea în dinamică a culturii de securitate.

Bibliografie:

1. BURCEA, C. și Hârțescu, I, *Manual de utilizare a social media în administrația publică*, Proiect finanțat prin granturile SEE, 2009-2014.
2. Comisia Europeană, *Journalists and Social Media*, Eurobarometer Qualitative Studies, 2012.
3. Legea privind statutul cadrelor militare, nr. 80, *Monitorul Oficial* nr. 155, București, 1995.
4. Legea privind protecția informațiilor clasificate, nr. 182, *Monitorul Oficial*, nr. 248, București, 2001.

5. Hotărâre pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România, nr. 585, Monitorul Oficial, nr. 485, București, 2002.
6. Legea privind siguranța națională a României, nr. 51, Monitorul Oficial, nr. 190, București, 2014.
7. Decizia nr. 4546/2014, Înalta Curte de Casație și Justiție, Secția de Contencios Administrativ și Fiscal.
8. Legea pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 31/2002 privind interzicerea organizațiilor și simbolurilor cu caracter fascist, rasist sau xenofob și a promovării cultului persoanelor vinovate de săvârșirea unor infracțiuni contra păcii și omenirii, nr. 217, Monitorul Oficial, nr. 558, București, 2015.
9. Legea pentru modificarea și completarea legii nr. 80/1995 privind statutul cadrelor militare, nr. 101, Monitorul Oficial, nr. 371, București, 2019.
10. https://ro.wikipedia.org/wiki/Rețea_de_socializare, accesat în 11.09.2019.
11. BRADLEY, P., „A New Definition of Social Media”, 2010, online: http://blogs.gartner.com/anthony_bradley/2010/01/07/a-new-definition-of-social-media/, accesat în 30.08.2019.
12. <https://en.wikipedia.org/wiki/Microblogging>, accesat în 30.08.2019.
13. https://en.wikipedia.org/wiki/Operations_security, accesat în 30.08.2019.
14. OECD, „Focus on Citizens, Public Engagement for Better Policy and Services”, 2009, online: <http://www10.iadb.org/intal/intalcdi/pe/2009/03785.pdf>, accesat în 30.08.2019.
15. URS Nicolae, *Folosirea social media în administrația publică din România*. Studiu Pilot, Departamentul de Administrație și Management Public, Facultatea de Științe Politice, Administrative și ale Comunicării, Universitatea Babeș-Bolyai, Cluj-Napoca, România, online: <http://rtsa.ro/rtsa/index.php/rtsa/article/download/501/498>, accesat în 30.08.2019.
16. Maj. BRENTON Pomeroy, „Time to Engage in Social Media”, Military Review website, March 23, 2017, online: <http://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Time-to-Engage-in-Social-Media/>, accesat în 30.08.2019.
17. Bitdefender ATP 28 Under the Scope, A Journey into Exfiltrating Intelligence and Government Information, 2015, online: www.download.bitdefender.com/resources/media/materials/white-papers/en/, accesat în 30.08.2019.
18. Social Media Posts Reveal NATO Soldiers' Activities, Report Says, 2019, online: <https://www.nytimes.com/2019/02/21/world/europe/nato-social-media.html>, accesat în 30.08.2019.
19. NABIE Y. Conteh, Paul J. Schmick, Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks, online: https://www.accentjournals.org/Paper_Directory/Journal/IJACR/2016/3/1.pdf, accesat în 30.08.2019.
20. Strategie națională cu privire la furtul de identitate în România în cadrul programului „Observatorul Național” model antifurt de identitate, online: <http://www.furtdeidentitate.ro/furtul-de-identitate/draft-strategie-nationala/>, accesat în 30.08.2019.
21. POLONSKAYA, Galina, Russia's Duma passes bill in first reading to separate its Internet system from global network, 2019, online: https://www.euronews.com/2019/02/12/russia-planning-to-disconnect-from-global-network-with-separate-internet-system?utm_source=newsletter&utm_medium=en&utm_content=russia-planning-to-disconnect-from-global-network-with-separate-internet-system&_open=eyJndWlkIjoIYTUyNTNhZTkxZWU0YTZhZGY2Y2VlYzcyNWl4Yzc2MzQifQ%3D%3D, accesat în 30.08.2019.
22. SUKHANKIN, Sergey, Another Step Forward Toward 'Sovereign' Russian Internet, 2019, online: <https://jamestown.org/program/another-step-forward-toward-sovereign-russian-internet/>, accesat în 30.08.2019.
23. Directiva 95/46/CE a Parlamentului European și a Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, online: <https://www.dataprotection.ro/servlet/ViewDocument?id=44>, accesat în 30.08.2019.
24. FERDINANDO, Lisa, “Soldiers Must Consider OPSEC When Using Social Media”, online: https://www.army.mil/article/103528/Soldiers_must_consider_OPSEC_when_using_social_media, accesat în 30.08.2019.

¹ https://ro.wikipedia.org/wiki/Rețea_de_socializare.

² P. Bradley, „*A New Definition of Social Media*”, 2010.

³ Microblogging - mediu de difuzare online care există ca o formă specifică de blogging. Un micro-blog diferă de un blog tradițional prin faptul că are un conținut de obicei mai mic, atât în dimensiunea reală, cât și în dimensiunea agregată a fișierului.

⁴ RuNet – site-uri web de limba rusă, găzduite în Federația Rusă.

⁵ OPSEC: proces care identifică informațiile critice pentru a determina dacă acțiunile prietenoase pot fi observate de inteligența inamică, determină dacă informațiile obținute de adversari ar putea fi interpretate pentru a le fi utile și apoi execută măsuri selectate care elimină sau reduc exploatarea adversă de informații critice prietenoase.

⁶ Legea 101/2019, art. 29, lit. c

⁷ *Hashtag*- cuvânt sau frază precedate de semnul #. A luat naștere pe 23.08.2007, pe rețeaua Twitter, fiind folosit de Chris Messina (co-fondator Uber).

⁸ Legea nr. 80/1995, art. 29.

⁹ Legea nr. 80/1995, art. 29, lit. b.

¹⁰ Legea 187/2012, art. 6¹.

¹¹ Legea 101/2019, art.29, lit.a.

¹² Codul Penal, art. 293.

¹³ Bitdefender – ATP 28 Under the Scope, A Journey into Exfiltrating Intelligence and Government Information.

¹⁴ C4ISR – prescurtare a sintagmei comandă, control, comunicații, computere, informații, supraveghere și cercetare.

ACȚIUNI ALE SERVICIILOR SECRETE ȚARISTE ÎN ROMÂNIA, ÎN EPOCA MODERNĂ

*Ioan-Codruț LUCINESCU**

Abstract

As early as the first decades of the 19th century, the Russian Empire gets actively involved, on a large scale, in actions meant to destabilize the Romanian society, by creating social and political disarray to prove to the public opinion on an international level that they're the only ones that could stabilize and help modernize the south-eastern part of the continent.

Russia's secret activity on Romanian territory in the modern age was complex and focused on knowing every detail of the political and economic aspect, on controlling, from an informational point of view, the main politicians, organizing attacks to get rid of the ones standing in the way of the imperial policy in the region etc.

Keywords: *espionage, Department for General State Security, Ministry of Interior, Romanian Army, Russian Empire.*

Mărturii din epocă despre acțiuni subversive ale Rusiei țariste pe teritoriul României

Încă din primele decenii ale secolului al XIX-lea, Imperiul țarist se implica activ și pe scară largă în acțiuni de destabilizare a societății românești, în crearea de convulsii sociale și politice, pentru a demonstra opiniei publice internaționale că numai Rusia poate avea un rol stabilizator și modernizator „la porțile Orientului”. Dintre numeroasele mărturii ale epocii, amintim pe cele legate de momentul revoluționar 1848 în Țara Românească, locul unde revoluția a și izbândit, din păcate doar pentru scurt timp.

Un fin observator al epocii, Grigore Zosima, reliefa într-o lucrare dedicată lui Grigore Scarlat Grădișteanu, lider revoluționar mai puțin cunoscut în istoriografia națională, rolul vital jucat de acesta în dejucarea unor acțiuni subversive inițiate de poliția secretă țaristă, în vara anului 1848, în București¹.

După abdicarea domnitorului Gheorghe Bibescu, la 13 iunie 1848, Grigore Scarlat

Grădișteanu, membru al unei ilustre familii boierești muntene, s-a implicat activ în transpunerea în practică a ideilor revoluționare, devenind un personaj important al mișcării pașoptiste. Lunile următoare au fost deosebit de agitate pentru guvernul provizoriu, pus în fața unor enorme provocări interne și externe, menținerea ordinii fiind vitală pentru succesul revoluției. Situația potențial explozivă în care se afla Capitala, cu posibile vărsări de sânge și convulsii sociale care ar fi fost pretextul perfect pentru intervenția armată a trupelor imperiilor vecine, a putut fi evitată prin stăruințele conducătorilor guvernului provizoriu, Ion Heliade Rădulescu, Gheorghe Magheru și Cristian Tell.

Grigore Scarlat Grădișteanu, la insistențele acestora, a ocupat postul de Director al Poliției Capitalei, poziție din care, cu ajutorul rețelelor de informatori răspândiți în toate mediile sociale, a reușit să anihileze acțiunile agenților serviciilor secrete ostile, în primul rând ale celor țariste și turcești. În activitatea informativă vitală pentru stabilitatea guvernului revoluționar, s-a bazat

**Expert în studii de securitate.*

pe preoții din mahalalele Bucureștiului, care cunoșteau în detaliu ceea ce se petrecea și, mai ales, ceea ce agitatorii trimiși atât de ruși, cât și de turci, puneau la cale. Astfel, se va evita, în august-septembrie 1848, o baie de sânge în București, în momentul în care trupele otomane erau deja la porțile orașului. Cuvintele lui Zosima, așa cum au fost ele consemnate în acele momente tulburi, bazate pe mărturiile pașoptiștilor bucureșteni, sunt relevante:

„Pote că demagogii (antirevoluționarii, n.n.) ar fi și ajuns să realizeze **dorința muscalilor** (subl. n.) dacă Heliade nu s-ar fi servit de tota influența lui ca să se mănție ordinea în Bucuresci prin amicii sei și prin neguțători, și în țară prin omenii tari de îngeri și chiar prin țărani. Ne aducem încă aminte de *cutreierările Grădișteanului prin mahalale ca să liniștească spiritele și să îndemne pe amici și inimi la pace și frăție*. Astă conduită făcișă pote să nu fi fost gustată de unii, dar el își împlinea datoria și jurământul ce făcuse ca să se opue cu orice preț la o rescolă. Era unul din vechii luptători. Împrejurările îl ajutaseră să se bucure de o mare popularitate și să fie în Bucuresci și chiar afară bine vedut și cunoscut. Bunul simț al românilor îi făcuse să-și cunoscă pe adevărații bine-voitori”².

Acest gen de acțiuni (de destabilizare a societății), specifice serviciilor secrete (indiferent că sunt civile, militare sau mixte), se vor amplifica în România în deceniile de final ale secolului al XIX-lea și început de secol XX, culminând cu răscoala țărănească din 1907. Deși în epocă subiectul implicării externe a fost trecut sub tăcere, printr-un acord tacit al clasei politice românești, nedorindu-se tensionarea și mai mult a relațiilor cu puternicul imperiu de la răsărit, dovezile conduc spre o concluzie evidentă: serioasele probleme sociale existente, fără îndoială, în satul românesc au fost exacerbate de agenți ai poliției secrete țariste și nu numai (interese în destabilizarea țării avea inclusiv aliatul nostru de atunci, Austro-Ungaria).

La începutul răscoalei, în primul său raport adresat conducerii statului, prefectul județului Botoșani, Jules Văsescu, solicita imperios, la 10 martie 1907, ca trupele ce vor fi trimise drept întăriri să fie unități de cavalerie, deoarece instigatorii nu provin din satele răsculate, ci se deplasează rapid, din sat în sat: „*sunt emisari care cutreeră satele și promit în numele MS Împăratul*

Rusiei de a împărți tot pământul la țărani și îi îndeamnă de a se revolta pentru a veni Rusia să domnească pe această țară, căci numai ei vor putea distribui pământul”³.

În al doilea raport al prefectului, datat 11 martie 1907, era reînnoită cererea de ajutor din partea armatei, deoarece situația se agrava rapid: „Faza revoluției s-a schimbat, locuitorii, grație instigatorilor – *se crede ruși de naționalitate* – ce cutreieră satele, văzând că au putut să-și îndeplinească pretențiunile lor către arendași și proprietari, cer mai mult: împărțirea pământurilor între ei...E necesitate absolută de cavalerie pentru a putea urmări cu folos bandele care cutreeră satele spre a răzvrăti locuitorii. Infanteria nu poate îndeplini această sarcină”⁴.

Deși în deceniile următoare s-a negat existența acestor instigatori (de diverse naționalități) ai serviciilor secrete țariste, este evident că Petrogradul încerca să profite din plin de orice problemă internă a României, guvernării țării știind foarte bine acest lucru. De aceea, începând cu 7 martie 1907, autoritățile române ordonă închiderea frontierei „începând de la Suceava până la Mihăileni” pentru a împiedica infiltrarea de agenți travestiți în țărani bucovineni și a nu oferi nici un pretext de intervenție militară din partea Rusiei țariste și Austro-Ungariei⁵.

De altfel, referiri la instigarea țăranilor de către agitatori profesioniști (anarhiști, socialiști etc.) au loc chiar în Parlamentul României, cu ocazia dezbaterilor pe marginea unor proiecte de legi necesare modernizării țării. Situația grea a țăranimii în Vechiul Regat, în general, era un fapt cunoscut și recunoscut, liberalii urmărind prin acte legislative să o amelioreze. Dar inițiativele lor privind crearea rețelelor rurale de bănci populare, cooperative sătești și alte instituții menite să asigure țăranilor acces la credit ieftin și sigur erau atacate vehement de conservatori.

Cu tot subiectivismul inerent poziției sale de mare moșier, Ion C. Grădișteanu, senator al Colegiului I, județul Râmnicu-Sărat, în discursul rostit în ședința Senatului din 20 decembrie 1907, prezintă aspecte interesante legate de izbucnirea și propagarea răscoalei:

„Că au fost instigațiuni, toată lumea o recunoaște; *felul chiar cum s-au dezvoltat răscoalele arată că erau cuvinte de ordine date, că era un sistem preconcept, un plan dinainte hotărât*. Într-adevăr, în toată Moldova s-a răsculat

țărâtimea cu același cuvânt de ordine: falcea 25 de lei; iar în toată Muntenia: dijma din zece una și izgonirea arendașilor. În afară de aceasta, au fost chiar amănunte de tactică cari dovedesc că această mișcare a fost condusă de cineva, de unul sau mai mulți capi (...).

Chiar răscoalele din astă-primăvară cu toții știm că au izbucnit din două părți: în Moldova din județul Iași, în Muntenia din județul Teleorman, adică din acele județe unde în 1898 s-a dat de urma instigatorilor socialiști. Și acum s-a dat de urma unor instigatori cari, în primul moment au și fost arestați de armată; la urmă însă au fost liberați înainte chiar de amnistie. Cînu nu știe, de pildă, că un anume Stoica Iorga, actualul primar al comunei Stănești din județul Vlașca, unde s-a întîmplat marea nenorocire cu locotenentul Nițulescu, a fost una din căpeteniile răscoalei și că, deși a fost arestat de armată, a fost liberat de prefect și astăzi este primar.

În județul Iași s-au găsit instigând *studenți basarabeni*, încă odată aștept dosarele, dar până la aducerea lor avem semne sigure cari ne călăuzesc”⁶.

Acțiuni de filaj desfășurate de serviciile de informații românești în vederea cunoașterii activității agenților ruși pe teritoriul național, la începutul secolului XX

Legea de reorganizare a Ministerului de Interne adoptată în aprilie 1903, în timpul mandatului ministrului Vasile Lascăr, s-a dorit a fi răspunsul la evoluția societății românești în acel început de secol; evenimentele ulterioare au demonstrat, însă, că aceasta era potrivită pentru instituția poliției doar ca „poliție administrativă”, lipsindu-i componenta informativă, cea de culegere a informațiilor necesare asigurării securității țării⁷.

Răscoala țărănească din martie 1907 a jucat rolul unui veritabil „duș rece” pentru elita politică românească, luată total pe nepregătite din cauza inexistenței unor informări pertinente despre situația explozivă înregistrată, în acel moment, în lumea rurală. De aceea, în martie 1908 este adoptată legea prin care apare Direcția Poliției și Siguranței Generale (DPSG) în cadrul Ministerului de Interne, având două secțiuni: cea a *Siguranței Generale a Statului* și cea a Poliției. Pentru asigurarea unei autonomii sporite, toate structurile cu atribuții de siguranță de stat au

fost organizate și au funcționat separat de Poliția Generală a Statului, fiind, astfel, mai puțin expuse presiunilor venite din partea autorităților locale, în frunte cu prefectul, sau partidelor politice aflate, vremelnic, la putere⁸.

Urmărind să creeze un organ de stat capabil să îndeplinească, profesionist, sarcini speciale, conducerea statului concepea *Siguranța Generală a Statului* ca „nervul poliției ce se impresionează la timp de mediul înconjurător (are capacitate informativă și contrainformativă adecvată pentru a acționa preventiv, n.n.), avizând la măsurile generale în materie de ordine publică și siguranța statului, înregistrând în același timp toate mișcările seismice ce se produc în populația internă cât și în țările înconjurătoare, pentru ca la timpul oportun să se poată preveni acele mișcări cu caracter subversiv contra siguranței statului”⁹.



Copertă a unui dosar de urmărire operativă (filaj) instrumentat de echipe ale Siguranței Statului (dosar aflat în fondul Arhivelor Naționale ale României). În document sunt descrise caracteristicile fizice (înălțime, constituție, semne particulare, culoare ochi și păr) ale celor cinci agenți ai poliției secrete ruse (Ohrana) despre care poliția de frontieră informase că se aflau pe teritoriul național. Descrierea a fost trimisă spre informare conducerii Direcției Poliției și Siguranței Generale și Marelui Stat Major al Armatei.

De asemenea, se acorda o mare importanță poliției de la punctele de frontieră și din porturi, aceasta aflându-se sub conducerea directă a ministrului de Interne și exercitată prin directorul DPSG, cel care avea dreptul de control deplin asupra întregii activități¹⁰.

În concluzie, Siguranța Statului, fiind, în acel moment, principala instituție de culegere a informațiilor pe plan intern și extern, avea obligația să asigure ordinea constituțională, securitatea internă a țării și să contracareze acțiunile întreprinse de statele ostile nouă, care ar fi atentat la independența și integritatea teritorială a României. Datorită faptului că Armata nu dispunea, încă, de un serviciu contrainformativ semnificativ, agenții Siguranței și ai Poliției din Capitală și din teritoriu desfășurau o intensă activitate inclusiv în folosul aparatului militar național, numeroase rapoarte „sensibile” fiind, transmise, în regim urgent și Ministerului de Război și Marelui Stat Major.

Strânsa colaborare între diferitele structuri ale instituțiilor statului (Ministerul de Interne și Armată, serviciul Poștei și Telegrafului etc.) a avut efecte pozitive notabile, prin descoperirea și anihilarea multor încercări ale diverselor puteri străine (Rusia țaristă, Austro-Ungaria, Germania etc.) de a cunoaște punctele tari, dar, mai ales, vulnerabilitățile României.

În cele ce urmează ne referim la acțiuni de supraveghere operativă (filaj) derulate de agenți ai serviciilor de informații naționale pentru depistarea, monitorizarea și „intoxicarea” informativă a unor rețele create, pe teritoriul României, de serviciul de spionaj al armatei imperiale ruse, în perioada premergătoare izbucnirii Primului Război Mondial.

„Personajul” principal al cazului prezentat este cetățeanul rus Vladimir Nicolaevici¹¹, care, pe parcursul a aproape doi ani (1913-1914), vine deseori în România, oficial pentru a-și crea relații în lumea bancară în vederea facilitării importului unor produse industriale rusești. Dar această acoperire ascundea un spion versat, cunoscător al spațiului est-european, datorită deselor călătorii în Bulgaria și Serbia.

În Referatul redactat de sub-directorul Siguranței Statului, Stan N. Emanuel, prezentat conducerii DPSG la 2 martie 1914¹², se arăta: „O latură a activității spionajului militar rus în România este serviciul de spionaj organizat

anume pentru Moldova, având sediul central în Odessa la Statul Major rus, circumscripția militară Odessa.... Legătura între Odessa și Iași se face de un oarecare Vladimir Nicolaevici, rus de origine, pretins comerciant, care vine foarte des în România și care era bănuț de mult timp că făcea spionajiu.

Din examinarea dosarului cu No. 227 din archiva secretă a Direcțiunei rezultă că acest Vladimir Nicolaevici.... s-a adresat avocatului Alexandrescu din Iași, făcându-i propunerea ca în schimbul unei sume de bani ce i se va servi lunar, să se intereseze el de activitatea acestor agenți (să devină coordonatorul rețelei de informatori pe care Nicolaevici o crease, anterior, n.n.), iar rapoartele lor să fie trimise la Odessa.

Advocatul Alexandrescu denunțând afacerea Direcțiunei și întrucât noi aveam interesul să cunoaștem felul informațiilor ce se cereau de ruși în chestiuni militare, precum și de a ști cine erau persoanele cari făceau asemenea servicii statului rus, am cerut avocatului Alexandrescu să primească propunerea”.

Astfel, prin avocatul Alexandrescu, devenit informator, atât Ministerul de Interne, cât și Armata vor cunoaște, în detaliu, modul de lucru și tipul de informații solicitate de spionajul ruses, civili și militari suspecti ca făcând parte din rețeaua lui Nicolaevici, alte vulnerabilități ale instituțiilor statului (în special pe zona de frontieră) de care serviciile secrete străine profitau etc. Dar acest avantaj evident nu scutește structurile informative ale Siguranței de a desfășura o amplă acțiune de supraveghere (filaj), care a necesitat efective sporite și un efort continuu timp de multe luni.

Agenții de filaj ai Siguranței îi înregistrează fiecare deplasare, inclusiv stările de spirit prin care trece spionul rus pe parcursul deselor deplasări în București: „mai sunt de remarcat iarăși așteptările lui însoțite de gesturi nervoase în diferite părți ale Capitalei, precum și staționarea lui în două rânduri în fața Școalei de artilerie și geniu, unde părea că așteaptă pe cineva. Întâlnirile în stradă și la locuri anumite cu femei de naționalitate rusă, între cari a putut fi recunoscută o anume Nadina, care este pusă și ea în supraveghere și despre care se face informațiune”¹³. Activitatea sa era febrilă, participând aproape zilnic la diverse întâlniri mai mult sau mai puțin conspirative.



În primele două decenii ale secolului XX, Biserica Rusă din Capitală a reprezentat unul din punctele de sprijin importante pentru serviciile secrete rusești¹⁴

Deosebit de interesant este schimbul de scrisori secrete din luna mai 1914, aflate în posesia structurilor informative naționale, între spionul rus și avocatul Alexandrescu din Iași. Spionajul militar țarist se arăta nemulțumit de lipsa de informații cu valoare reală furnizate de român (documentele predate spionului rus erau elaborate de Alexandrescu sub îndrumarea Siguranței Generale a Statului). Nicolaevici este foarte clar în acest sens: „Ultimele d-tale scrisori conțin numai informațiuni politice generale ... de astfel de informațiuni n-avem nevoie... Nouă ne trebuie numai informațiuni militare... Trebuie ca d-v să faceți imediat cunoștințe printre militarii corpurilor stabilite în Iași, pentru ca prin aceste cunoștințe să aflați totul despre viața regimentelor și să ne scrieți despre toate... D-v trebuie să ne comunicați toate informațiunile despre armata română... despre schimbarea organizării armatei și despre formarea unităților noi... despre marină, despre comenzi de tunuri, îmbrăcăminte, puști, proiectile etc.”¹⁵.

I se cerea avocatului ca aceste informații să fie cât mai detaliate, spionajul rus fiind interesat inclusiv de eventuale nereguli financiare înregistrate la unitățile românești, numele ofițerilor pedepsiți disciplinar, incidente între

ofițeri, datorii ale acestora la jocuri de noroc etc. Reamintim faptul că acest gen de informații focalizate pe viața cotidiană a ofițerilor a dus la racolarea, la începutul secolului XX, a colonelului austriac Alfred Redl, șeful secției contraspionaj din cadrul serviciului de informații al armatei imperiale austro-ungare (1907-1912), acțiune de mare succes a serviciilor secrete ruse (meritul revenindu-i colonelului Nikolai Batyushin), cu urmări catastrofale pentru monarhia austro-ungară în timpul primei conflagrații mondiale.

Concret, spionajul militar țarist îi solicita avocatului Alexandrescu, devenit principalul agent al rețelei lui Nicolaevici, să se infiltreze în cercul ofițerilor garnizoanei Iași pentru a afla informații detaliate și cu posibil impact de trădare: „(...) despre incidentele dintre ofițeri, despre pedepsele suferite de ofițeri, despre nereguli bănești semnalate la Corpuri de armată etc. Aceste chestiuni sunt foarte importante pentru noi. D-v trebuie să ne comunicați toate informațiunile despre armata română. Cele mai importante pentru noi sunt: 1) Despre schimbarea organizării armatei și despre formarea, înființarea unităților noi; 2) Despre mutarea trupelor; 3) Despre schimbarea de efectiv a corpurilor; 4) Despre marină; 5) Despre comenzi de tunuri, îmbrăcăminte, puști, proiectile etc... Când ne comunicați informațiuni trebuie să ne dați detațiuni pentru fiecare chestiune, ex: Când vorbiți despre formarea unităților noi, trebuie să ne arătați exact, unde când și cum vor fi formate trupele acestea. Când comunicați despre comenzi, trebuie să arătați când, unde și câte comenzi s-au făcut (tunuri, proiectile, muniții și când sunt gata)”¹⁶.

Deoarece avocatul Alexandrescu era, așa cum am amintit, agent al Siguranței, autoritățile române au putut controla rețeaua de spionaj, pe această filieră scurgerile de informații „secret militar” către centrul rus din Odesa fiind nesemnificative. Totuși, acțiunile de „intoxicare” nu erau nici pe departe simple și facile, deoarece spionajul militar rus dispunea și de alte persoane, civili și ofițeri, care îi furnizau informații (adevărate de această dată) despre procesul de adaptare al armatei române la realitățile internaționale din vara lui 1914.

Urmărirea activității lui Vladimir Nicolaevici în București pe parcursul lunilor mai-august 1914 (în această perioadă urmărirea s-a intensificat, determinată fiind de pregătirile de război ale statelor europene) a presupus un efort logistic important din partea agenților echipelor de filaj, datorită necesității ca și persoanele cu care acesta interacționa frecvent să fie, la rândul lor, supravegheate. Unele dintre acestea, fiind ofițeri, au fost semnalate autorităților militare, care au trecut, prin structurile contrainformative ale armatei, la identificarea intențiilor lor și a informațiilor militare la care aveau acces; totuși, din filele dosarelor de urmărire nu reiese dacă acești militari i-au livrat secrete de serviciu sau doar făceau parte din cercul larg de cunoscuți pe care „omul de afaceri” rus îl avea în țara noastră.

De exemplu, echipa de filaj care se afla la post pe 25 mai 1914 raportează faptul că Nicolaevici se întâlnește la Cafe Bristol cu doi români, dintre care unul era militar (locotenent de artilerie), identificat în persoana lui Popescu Vintilă, din garnizoana Pitești. Agentul 76 din Brigada I a Siguranței notează în raport: „Astă noapte la ora 1^{1/2} pe când mă retrăgeam din supraveghere am văzut pe str. Academiei colț cu Bulevard pe cunoscutul rus Vladimir Nicolaevici care locuiește în str. Scaune 17 și care a fost mai mult timp supravegheat, însoțit fiind de un domn locotenent de artilerie și un alt tânăr cu care au intrat în Cafe Bristol. Din informațiunile ce am putut culege prin chelnerul ce îl servea am putut afla că locotenentul se numește Popescu Vintilă și precum se înțelegea din discuția ce au avut-o părea că acel ofițer este din provincie. La ora 3 l-au condus pe Vladimir Nicolaevici acasă în str. Scaune 17 iar cei 2, locotenentul și tânărul s-au dus pe str. Scaune traversând Bulevardul și în fundătura teilor nu i-am mai văzut, probabil au intrat într-o casă”¹⁷.

Operațiunea de supraveghere a continuat încă câteva luni, prin Nota din 6 august 1914 a Brigăzii de Siguranță Galați conducerea DPSG fiind informată despre plecarea acestuia din țară: „Astăzi 6 august a.c., ora 8 a.m. a plecat din hotel s-a dus la Agenția Rusă și s-a îmbarcat pe vaporul rusesc pentru Odesa, până la debarcader a fost condus de ziaristul rus Ilios Gorelik... Din supravegherea făcută asupra lui V. Nicolaevici nu s-a observat nimic suspect”¹⁸.

Dosarele Siguranței nu îl mai consemnează din acel moment, locul său fiind însă luat de alți „oameni de afaceri” ruși, printre care Vladimir Caminski, spion pentru care România va deveni, în anul 1915, o a doua casă prin timpul petrecut în București, Sinaia, Predeal, Constanța etc.

Concluzii

Vladimir Nicolaevici este doar unul din sutele de cazuri de spioni aparținând Rusiei țariste, Germaniei, Austro-Ungariei, Bulgariei, Turciei etc. instrumentate de sistemul național de securitate în preajma izbucnirii Primului Război Mondial, moment în care importanța politică și militară a României a crescut semnificativ în ecuația de putere europeană; țara noastră devenind, în cei doi ani de neutralitate (iulie 1914 – august 1916), o veritabilă placă turnantă a serviciilor secrete ale puterilor beligerante, atât Antanta, cât și Puterile Centrale urmărind să o determine să intre în război de partea sa.

Activitatea secretă a Rusiei țariste pe teritoriul românesc a fost una complexă și focalizată pe cunoașterea în detaliu a vieții politice și economice naționale, pe „controlul informativ” al oamenilor politici importanți și pe organizarea de atentate în vederea eliminării persoanelor incomode pentru politica imperială în regiune etc.

Notăm faptul că agentura secretă rusă s-a sprijinit, în special după anul 1878, și pe elemente aparținând puternicei minorități slave, existentă deja de generații pe teritoriul național (în special în zona Deltei Dunării și Dobrogea); în plus, odată cu demararea procesului de modernizare al societății românești și oportunitățile ce decurgeau de aici, se înregistrează un mare număr de „supuși ruși” de diverse etnii veniți în țara noastră, în mod oficial, în căutarea unei vieți mai bune și pentru a scăpa de represiunea autorităților țariste.

Bibliografie:

1. Arhivele Naționale ale României, Fond Direcția Generală a Poliției.
2. BACALBAȘA Constantin, Bucureștii de altădată, vol. III, Editura Albatros, București, 2000.
3. BOBOCESCU Vasile, Istoria Poliției Române, Editura Ministerului de Interne, București, 2000.

4. GRĂDIȘTEANU Ion C., Discurs rostit în ședința Senatului din 20 decembrie 1907, Imprimeria Statului, București, 1908.
5. POHRIB Adrian, Din istoria Poliției Române. Poliția orașului Galați între anii 1832 și 1949. Istoric și documente, Editura AGATON, Galați, 2013.
6. SPÂNU Alin, Serviciul de informații al României în războiul de întregire națională (1916-1920), Editura Militară, București, 2012.
7. STOENESCU Alex Mihai, Istoria loviturilor de stat în România, vol. 2, Editura RAO, București, 2001.
8. ȘTEFĂNESCU Paul, Istoria serviciilor secrete române, Editura ANTET, Prahova, 2007.
9. ZOSSIMA Grigore, Biografii politice ale oamenilor mișcării naționale din Muntenia la 1848, Tipografia N. Minulescu, București, 1884.

¹ Grigore Zossima, *Biografii politice ale oamenilor mișcării naționale din Muntenia la 1848*, Tipografia N. Minulescu, București, 1884, pp. 5-8, Biblioteca Academiei Române.

² Ibidem, p. 30.

³ *Răscoala din 1907*, vol. I, Editura de Stat, București, 1948, p. 49, apud Alex Mihai Stoenescu, *Istoria loviturilor de stat în România*, vol. 2, Editura RAO, București, 2001, p.134.

⁴ Ibidem, p. 54 (Raportul nr.1933 din 11 martie 1907), apud Alex Mihai Stoenescu, op. cit., p.134-135.

⁵ Alex Mihai Stoenescu, op. cit., p.131.

⁶ Ion C. Grădișteanu, *Discurs rostit în ședința Senatului din 20 decembrie 1907*, Imprimeria Statului, București, 1908.

⁷ Adrian Pohrib, *Din istoria Poliției Române. Poliția orașului Galați între anii 1832 și 1949. Istoric și documente*, Editura AGATON, Galați, 2013, p.63.

⁸ Alin Spânu, *Serviciul de informații al României în războiul de întregire națională (1916-1920)*, Editura Militară, București, 2012, p.27.

⁹ Vasile Bobocescu, *Istoria Poliției Române*, Editura Ministerului de Interne, București, 2000, p.141.

¹⁰ Adrian Pohrib, op. cit., p.64.

¹¹ Rețeaua de spionaj creată de Nicolaevici în România este prezentată, detaliat, în Ioan Codruț Lucinescu, *Din culisele spionajului rus pe teritoriul României, la începutul secolului XX*, Revista Română de Studii de Intelligence (RRSI), nr. 11, 2014.

¹² Arhivele Naționale ale României, Fond *Direcția Generală a Poliției*, Dosar nr. 1/1914, file 30-32.

¹³ Ibidem, fila 32.

¹⁴ <http://www.bucurestiivechisinoi.ro/2011/03/biserici-bucurestene-i/>; în prezent se află pe Strada Blănari, nr. 16.

¹⁵ Arhivele Naționale ale României, Fond *Direcția Generală a Poliției*, file 97-97v.

¹⁶ Ibidem.

¹⁷ Ibidem, fila 111.

¹⁸ Ibidem, fila 199.

