UA: UKRAINE ANALYTICA

Issue 3 (21), 2020

- PANDEMIC RESPONSE
- INFODEMIC AND STRATEGIC COMMUNICATIONS
- SECURITY STRATEGIES

UA: UKRAINE ANALYTICA

Issue 3 (21), 2020

New Threats

Editors
Dr. Hanna Shelest
Dr. Mykola Kapitonenko

Publisher:
Published by NGO "Promotion of Intercultural Cooperation" (Ukraine), Centre of International Studies (Ukraine), with the financial support of the Representation of the Friedrich Ebert Foundation in Ukraine, the Black Sea Trust.

UA: Ukraine Analytica is the first Ukrainian analytical journal in English on International Relations, Politics and Economics. The journal is aimed for experts, diplomats, academics, students interested in the international relations and Ukraine in particular.

Contacts:
website: http://ukraine-analytica.org/
e-mail: Ukraine_analytica@ukr.net
Facebook: https://www.facebook.com/ukraineanalytica
Twitter: https://twitter.com/UA_Analytica

ISSN 2518-7481

500 copies

BOARD OF ADVISERS

TABLE OF CONTENTS

HYBRID WARFARE AS A THREAT TO INTERNATIONAL SECURITY

Margarita Biryukova
LL.M. (Europa-Institut, Saarbrucken, Germany)

In the 21st century, states employ concealed ways to destabilise adversaries and achieve geopolitical goals, thus resorting to hybrid warfare. This may include economic pressure, interference in political affairs, cyber-attacks, disinformation, and other means. Considering the most recent manifestations of hybrid warfare between states, the dilemma is how to build nations' resilience to such threats. Additionally, international law does not have a robust system to face the contemporary threat of hybrid warfare. This paper focuses on hybrid warfare, drawing on the example of the conflict between the Russian Federation and Ukraine, and analyses it from the international law perspective.

Introduction

The notions of war and peace are blurred. Understanding of peace as the absence of military conflicts is obsolete, since confrontations have moved into a different dimension. Pursuing strategic interests, destabilising adversaries, or achieving subordination of certain states can be completed in a concealed way without an armed attack.

With a rapid development of technology, it has become possible to launch a harmful attack against an enemy via the internet. Cyber-attacks can cause damage on a large scale. Information and political contexts can be turned into a weapon and used against a rival. Similarly, economy and trade can become a powerful leverage in shaping international relations. These are the means of modern mode of war, which is hybrid warfare. International reputation of states plays an important role in international relations, and wrongdoings of states can make them accountable. In such an environment, hybrid warfare offers a perfect solution. In a nutshell, lately the character of conflicts has evolved into a combination of physical and psychological means where even non-combatants play a role.[1]

Hybrid warfare tools may include a combination of various means, such as information war, propaganda, political and economic pressure, cyber-attacks, and usage of proxies. With the variety of means of war, it is rather impossible to give an exhaustive list of weapons used in hybrid war. Any measure that is able to shape political discourse in a particular manner, inflict fear, spread panic, work as a provocation, produce a desired public opinion, or distort public order can and will be used by a state waging hybrid warfare against the other. Therefore, even military exercises at the borders with another state, active militarisation of illegally annexed territories, movement of military units to the border with another state, and performance of combat readiness

1 F. Hoffman, *Hybrid Warfare and Challenges*, "Joint Force Quarterly", January/March 2009, p. 34.

checks should be regarded as components of a wider framework of hybrid war.

The primary target in hybrid warfare is the population, which is different from a traditional war, where the main targets are military forces and infrastructure. Targeting the minds of the adversary's population through information war is highly damaging, because grievances within a country can undermine security, discredit the government, and cause widespread distrust towards the regime. The effects of an outburst from within a country are long-lasting.

> ***military exercises at the borders with another state, active militarisation of illegally annexed territories, movement of military units to the border with another state, and performance of combat readiness checks should be regarded as components of a wider framework of hybrid war***

The annexation of Crimea by the Russian Federation in 2014, which was rapidly and bloodlessly executed, attracted attention. It was illegal from international law perspective and condemned by the majority of nations but has become a vivid case of hybrid warfare. Since the annexation, the term "hybrid warfare" is being frequently used in the security discourse. From the analytical point of view, hybrid warfare provides an interesting subject to study due to its multi-vectoral manifestation. Russia's hybrid warfare against Ukraine is an example of that.

Cyber Warfare

Cyber warfare became a concern to international security at the end of the 20th century; then, after being dormant for some time, it re-entered the security agenda following a series of damaging cyber-attacks against Estonia in 2007.[2] Due to the scale, it has become one of the most notorious attacks. Additionally, there were other cases of cyber-attacks in 2008 in Lithuania and Georgia. Each case had a political context to it, where cyber-attacks played a role of expressing discontent. In Estonia, the government made a decision to demolish a Soviet-era monument devoted to World War II, which provoked unrests from the side of ethnic Russian population and triggered outrage in the Russian government.[3] In the Lithuanian case, the government of Russia vocally condemned the amendment to the national Lithuanian law that forbade public display of Nazi German and Soviet symbols as well as playing Nazi and Soviet anthems at public meetings.[4] In Georgia, cyber-attacks were coordinated with the timing of the military invasion by the Russian Federation into South Ossetia.[5]

In the Estonian case, it has been identified that some cyber-attacks in the wider cyber campaign came from Russian IP addresses, including ones belonging to state institutions.[6] According to iDefense, a security intelligence firm in the US, possibly

2 M. N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, "Stanford Law & Policy Review", June 2014, p. 269.

3 E. Tikk, K. Kaska, L. Vihul, *International Cyber Incidents: Legal Considerations*, Cooperative Cyber Defense Centre of Excellence: Tallinn 2010, p. 15.

4 Ibid., p. 51.

5 Ibid., pp. 67-68.

6 I. Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, "The Guardian", 17 May 2007 [www.theguardian.com/world/2007/may/17/topstories3.russia access: 6 July 2020].

nationalist Russian hackers executed the attacks in Lithuania, owing to the participation of a popular website of Russian hackers in the organisation of the cyber campaign.[7] In the Georgian case of a massive cyber campaign, instructions written in Russian on how to conduct cyber-attacks were shared on Russian-speaking websites, forums, and blogs, similarly to the situation in Estonia.[8]

Ukraine's cyber space has fallen victim to numerous cyber-attacks. Similarly to the Russian military invasion of Georgia, the annexation of Crimea by Russia was timed with a cyber-attack that shut down governmental websites in Ukraine and hacked cell phones of the members of the Parliament of Ukraine.[9] The Central Election Commission of Ukraine website was infected with malware on several occasions before elections were to take place. In the winter of 2015 and 2016, Ukrainian power grid experienced major cyber-attacks that deprived the population of electricity for many hours.

The climax of Russia's cyber war was the NotPetya attack, which is considered the world's most damaging cyber operation in history, according to Dr. Kenneth Geers, NATO Cyber Centre ambassador. The malware was unleashed in June 2017, on the day preceding Ukraine's Constitution Day, primarily infecting systems of financial institutions and causing catastrophic loss of data. Moreover, it shut down ministerial, postal services', and telecommunication companies' websites. The cyber operation affected the systems of the Kyiv international airport, Chernobyl site, energy companies; it impaired the functioning of Kyiv metro, ATMs, and card payment systems. This cyber-attack was a nationwide disaster that paralysed the country and then spilled over to other large businesses around the globe. The NotPetya operation, along with other cyber-attacks in Ukraine in 2015-2016, was attributed to the Kremlin-linked group of hackers known as Sandworm.[10]

Information Warfare

Information war is not novel in the 21st century. The traces of manipulation of public consciousness date back to World War I, when political leaflets were widely distributed.[11] The Cold War provides another good example of an intense, strategically powerful, and protracted information war.[12] Nowadays, with the reliance on the internet, being disinformed has become easy as never before. A single image with a piece of news shared on social media, regardless of whether the news is accurate or the picture is original, can influence opinions of many citizens. The information flow that every individual is exposed to can be overwhelming, where false information is easily mingled with facts. This makes public opinion an easy target for manipulation.

It is suggested that in 2013, the Russian focus shifted from mere cyber-attacks to conducting information operations, because

7 E. Tikk, K. Kaska, L. Vihul, n. 3, p. 55.

8 Ibid., p. 73.

9 T. Maurer, *Cyber Mercenaries. The State, Hackers, and Power*, Cambridge University Press: Cambridge 2018, p. 98.

10 A. Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, "Wired", 22 August 2018 [https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ access: 18 July 2020].

11 G. Pocheptsov, *Психологические войны (Psychological Wars)*, Vakler: Kyiv 2002, p. 42.

12 Ibid., p. 473.

from the Russian perspective, information manipulation performed by the West in the post-Soviet countries proved to be an effective tool.[13] This shift is attributed to the emergence of the so-called Gerasimov Doctrine, which is considered the blueprint of hybrid warfare.[14] This new Russian strategic focus reflects visibly in Ukraine's information space. Disinformation and pro-Kremlin propaganda are spread widely on social media through the Kremlin's trolls, who use fake accounts.[15] Every day hundreds of trolls have a goal of posting more than a hundred comments, and since the autumn of 2013 their activity has intensified.[16] This coincides with the time of the EuroMaidan demonstration in Kyiv.

Hybrid warfare does not exclude a military conflict taking place in parallel. In fact, information warfare has become a supplement to an armed conflict. The conflict between Russia and Ukraine in Donbas is surrounded by a disinformation campaign. It is worth recalling that when the conflict in eastern Ukraine broke out, international public believed that Ukraine was going through a civil war, despite Russia's involvement in this conflict. It is now known to the international community that not only was the separatist movement in eastern Ukraine fomented by the Kremlin, but the separatists were also supported by Russia through financing, training, and provision of arms through the notorious "humanitarian convoys". Typically for hybrid warfare, such an involvement was under the guise of a secessionist movement of Donbas from Ukraine.

Hybrid warfare does not exclude a military conflict taking place in parallel. In fact, information warfare has become a supplement to an armed conflict

Russia's annexation of Crimea was also accompanied by an active dissemination of disinformation. Studies show that Wikipedia articles regarding these events were massively edited to convey Russian propaganda.[17] The central messages of this propaganda included the narratives that the turmoil in Ukraine was caused by the Ukrainian authorities and the West, the Russian Federation is attempting to calm tensions, and the Kremlin needs to protect Russian speakers of different nationalities residing in various countries.[18]

Economic and Political Warfare

Ukraine's dependence on energy supplies from Russia has backfired in many cases. Since Ukraine gained independence in 1991, the Russian Federation has attempted to keep Ukraine as a satellite state; hence,

13 T. Maurer, n. 9, p. 61.

14 Ibid., p. 61.

15 D.-E. Mitu, *Information and Hybrid Warfare: Intelligence Challenges, Intelligent Response*, [in:] N. Iancu et al. (eds.), *Countering Hybrid Threats: Lessons Learned from Ukraine*, IOS Press: Amsterdam 2016, p. 62; A. Chen, The Agency, "New York Times Magazine", 2 June 2015 [https://www.nytimes.com/2015/06/07/magazine/the-agency.html access: 16 July 2020].

16 T. Maurer, n. 9, p. 61.

17 G. Pakharenko, *Cyber Operations at Maidan: A First-Hand Account*, [in:] K. Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications: Tallinn 2015, p. 62.

18 D.-E. Mitu, *Information and Hybrid Warfare: Intelligence Challenges, Intelligent Response*, [in:] N. Iancu et al. (eds.), *Countering Hybrid Threats: Lessons Learned from Ukraine*, IOS Press: Amsterdam 2016, p. 61.

it used oil and gas prices as a leverage.[19] Russia threatened to raise oil prices and terminate gas supply to Ukraine on some occasions when Ukraine's political decisions were unfavourable to the Russian government or political concessions from Ukraine were needed to achieve Russia's objectives. These occasions surrounded the following developments: Ukraine's decision to leave the ruble zone, rejection of Russia's territorial claim over Crimea, clashes connected to the Black Sea Fleet ownership, and Russia's pressure to force Ukraine to dismantle Soviet-era nuclear weapons on its territory.[20]

Construction of the Nord Stream 2 gas pipeline is a continuation of the gas saga between Russia and Ukraine. This gas pipeline will have a sizeable impact on Ukraine. Firstly, it will deprive the country of the transit fees due to the fact that the pipeline will bypass Ukraine. Russia's allegations that Ukraine breached its transit obligations, which would create an objective reason to exclude Ukraine from the transit route, were not supported by evidence. Secondly, and more importantly, it will allow Russia to halt gas supply to Ukraine anytime without affecting the EU states. The recent example of such a practice was in 2009, when Russia discontinued gas supply to Ukraine in order to exert political pressure. The existence of Nord Stream 2 will mean that Russia's threats or actual termination of gas supply to Ukraine will remain as leverage in political or any other context.

The notorious Kerch Strait Bridge, built by the Russian Federation despite the EU and US sanctions and Ukraine's objections, has resulted for Ukraine in economic losses. The height of the bridge obstructs traffic of large international vessels in the Azov Sea headed to the Ukrainian ports. The cargo of these vessels comprised 43% of all cargo handled by Mariupol port.[21] Smaller cargo vessels that are able to pass under the bridge are subjected to unlawful inspections by Russian authorities, causing undue delays. Moreover, by reducing the allowed length of vessels permitted in the Kerch Strait, Russian authorities have again exceeded the powers and added another instrument to the economic warfare. Although it is impossible to present evidence that the primary goal of this bridge was to damage Ukraine's economy, the construction of the bridge did play a role in a wider framework of hybrid warfare, especially bearing in mind that economic pressure in a globalised world is an immediate alternative to the use of force.[22] It is worth mentioning that from the initial stages of the Kerch Strait Bridge construction, it was declared that it violates Ukraine's sovereignty and territorial integrity, the UN Convention on the Law of the Sea, and a bilateral treaty between Russia and Ukraine on the Azov Sea and Kerch Strait.

---

19 F. Hill, P. Jewett, *Back in the USSR*, John F. Kennedy School of Government, Harvard University, January 1994, p. 66; F. Coldea, *Building National Capabilities and Countering Hybrid Threats: Lessons Learned*, [in:] N. Iancu et al. (eds.), *Countering Hybrid Threats: Lessons Learned from Ukraine*, IOS Press: Amsterdam 2016, p. 13; C. Eremia, *Main Features of the Hybrid Warfare Concept*, [in:] N. Iancu et al. (eds.), *Countering Hybrid Threats: Lessons Learned from Ukraine*, IOS Press: Amsterdam 2016, pp. 18-9.

20 F. Hill, P. Jewett, *Back in the USSR*, John F. Kennedy School of Government, Harvard University, January 1994, pp. 70-81.

21 *Обмеження для суден, які встановлює РФ, суперечать Конвенції ООН з морського права (Restrictions on Vessels Imposed by the Russian Federation Contradict the UN Convention on the Law of the Sea)*, Ministry for Reintegration of Temporarily Occupied Territories of Ukraine, 2017 [www.mtot.gov.ua access: 16 July 2020].

22 S. D. Ducaru, *Framing NATO's Approach to Hybrid Warfare,* [in:] N. Iancu et al. (eds.), *Countering Hybrid Threats: Lessons Learned from Ukraine*, IOS Press: Amsterdam 2016, p. 6.

Hybrid Warfare versus International Law

As has been demonstrated above, hybrid warfare is a sophisticated phenomenon comprising various elements. Despite the fact that hybrid threat is gaining prominence on the international security agenda, it is still challenging to coin an internationally accepted definition of this term. Legal remedies under international law do not grasp the whole picture and magnitude of hybrid war. Addressing separate instruments used in hybrid warfare would not suppress this type of war, as the aggressor can exploit other fronts to continue destabilising the target—even more so if the aggressor uses a fusion of capabilities in a synchronised campaign to achieve confusion and ambiguity.[23]

> ***Hybrid warfare is characterised by the aggressor's denial of involvement and accountability for its actions in another state, and further attempts to legitimise its actions, bending the norms of international law.***

If looking solely at the cyber aspect of hybrid warfare, it becomes clear that there are promising developments in this field. Considering modern threats to international security via network, international organisations aim at building robust cyber security strategies and work on confidence-building measures. Growing attention to cyber threats will stimulate development of technological capabilities to enhance cyber resilience.

The series of cyber-attacks on Estonia in 2007 opened up a discussion on whether international law is applicable to cyber space and whether a cyber-attack violates a state's sovereignty. The International Group of Experts working on the *Tallinn Manual on the International Law Applicable to Cyber Warfare* concluded that cyber space is indeed under the state sovereignty. The landmark International Court of Justice (ICJ) *Nuclear Weapons Advisory Opinion* of 1996 suggests that any use of force, irrespective of the weapon used, is unlawful under the UN Charter.[24] Yet, it is not that straightforward to apply this principle to cyber-attacks. It is hard to trace the origin of cyber-attacks and even harder to find substantial evidence that would prove a link between a state and culprits to attribute the attacks to the state. In addition, Article 51 of the UN Charter envisages individual or collective self-defence only in case of an armed attack.[25] This demonstrates the absence of available remedies for states-victims of cyber warfare. Even if the *Tallinn Manual* suggests that states may apply countermeasures to cyber operations, international law does not provide guidance in this respect and there is no state practice.

Despite the capability of hybrid warfare to avoid open military aggression, there are international documents that address this type of war. The ICJ judgment in the case *Nicaragua v. United States* held that encouraging, financing, arming, and training of anti-government forces in another country is in breach of the principle of non-intervention in internal affairs of the other

23 Ibid., p. 4.

24 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, [1996] ICJ Rep 1996, para. 39.

25 Charter of the United Nations and Statute of the International Court of Justice, San Francisco 1945, Article 51.

state.[26] The UN General Assembly (UNGA) Resolution 2625 (XXV), the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States, prohibits supporting, fomenting, inciting, or assisting terrorist or armed activities that aim at overthrowing a regime or intervene into civil conflict of another state. The UNGA Resolution 2131 (XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, explicitly prohibits direct and indirect intervention in internal and external affairs of the other state, and usage of political, economic, and other types of measures with the purpose of coercing the other state into subordination or receiving any advantages from it. These resolutions cover many tools of hybrid warfare and thus shape the principles of customary international law, but do not possess binding force and rely on states' good faith.

Needless to say, waging hybrid warfare goes against the fundamental principle of state sovereignty. The Permanent Court of Arbitration in the Island of Palmas case established: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State".[27] Independence and sovereignty of Ukraine were upheld in the Budapest Memorandum of 1994, signed by the UK, the US, Russia, and Ukraine as a security guarantee for Ukraine after the country's accession to the Treaty on the Non-Proliferation of Nuclear Weapons. Ironically, one of the parties to this treaty, namely the Russian Federation, became the state infringing on Ukraine's sovereignty and independence.

Hybrid warfare is characterised by the aggressor's denial of involvement and accountability for its actions in another state, and further attempts to legitimise its actions, bending the norms of international law. This is well demonstrated by the takeover of Crimea. The annexation started with "little green men", with no insignia, entering Crimea and seizing the administrative buildings and military sites. On 17 April 2014, President Putin admitted that the "little green men" were in fact Russian military.[28] The Kremlin played a card of legitimising its actions in Crimea: It was claimed that Russians were in danger and Russia had to militarily intervene to protect them on the basis of the Russian Military Doctrine[29], which was authorised by the Federation Council[30]. This stirred a debate regarding people's self-determination and secession provided in international law, which in reality was irrelevant for the Crimean case. Residents of Crimea did not belong to a distinct people entitled to self-determination; the evidence of discrimination or abuse of human rights

26 ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)*, Merits, [1986] ICJ Rep 1986, para. 292.

27 PCA, *The Island of Palmas Case (or Miangas) (USA v The Netherlands)*, Award (4 April 1928), p. 8.

28 *Putin Admits Russian Forces Were Deployed to Crimea*, "Reuters", 17 April 2014 [https://uk.reuters.com/article/russia-putin-crimea/putin-admits-russian-forces-were-deployed-to-crimea-idUKL6N0N921H20140417 access: 16 July 2020].

29 *Военная доктрина Российской Федерации (Military Doctrine of the Russian Federation)*, Ministry of Foreign Affairs of the Russian Federation, 2014 [https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589760 access: 16 July 2020].

30 *Об использовании Вооруженных Сил Российской Федерации на территории Украины (On the Use of Armed Forces of the Russian Federation on the Territory of Ukraine)*, Federation Council of the Federal Assembly of the Russian Federation, 1 March 2014 [http://council.gov.ru/activity/documents/39979/ access: 18 July 2020].

of Crimea's population was never presented by Russia; and self-determination and secession movement was not initiated by the population itself, but by the Russian military, which resembles an occupation. The referendum in Crimea, orchestrated by the Kremlin, was another effort to legitimise its annexation of the peninsula. It looked legal on the surface, but the result of this referendum was declared illegal by the international community, because it was against the Ukrainian national law and was conducted with the presence of Russian troops.

Although in theory hybrid warfare violates fundamental principles of international law, adjusting international legal norms to hold states accountable for this warfare is practically impossible. Hybrid warfare lacks clarity to identify all its forms, impose a threshold of violence to tailor international law, and hold states responsible. The main challenge stems from the core purpose of hybrid warfare of keeping the aggression covert, so that it does not amount to the threat or use of force under Article 2(4) of the UN Charter. Therefore, mass international condemnation and the imposition of sanctions are the only ways to counter hybrid threats.

Conclusion

Since 1991 the Kremlin has been demonstrating that Ukraine is in Russia's "sphere of influence", which precludes Ukraine's aspirations and plans to build close ties with the West. Russia's intention to keep Ukraine under its control implies intervening in Ukraine's internal affairs. Political moves that would bring Ukraine closer to the EU or NATO trigger the intensification of Russia's hybrid warfare, be it pulling economic or political leverages to undermine Ukraine's reliability. The main goal of hybrid warfare waged by Russia is destabilising Ukraine to prevent its potential memberships in the EU and NATO.

It is important for the Russian Federation from the strategic and geopolitical point of view to keep Ukraine as a puppet state: Ukraine has been a buffer zone between Russia and the EU, particularly NATO states. The first attempt to sign the EU-Ukraine Association Agreement was thwarted by Ukraine's pro-Russian former president. This triggered demonstrations to express people's pro-EU choice, but it also provided an opportunity for Russia to unfold full-scale hybrid warfare against Ukraine.

Waging hybrid warfare means resorting to "smart war". Hybrid war has considerable advantages over the conventional one. First, it allows one to attack an adversary from numerous fronts, which makes predicting an attack impossible. Hybrid warfare entails all possible instruments to pressure and manipulate the target. Second, the use of the internet in waging war makes hybrid warfare cost-efficient. Third, hybrid war is less damaging to the aggressor's international reputation. In an open armed attack, it is easier to identify the state-aggressor, whereas using hybrid methods allows the perpetrator to stay unidentified and deny any responsibility. Fourth, methods of hybrid warfare bypass the norms of international law and render states-victims with no protection. Such countries can only work on their resilience to this threat. Ultimately, it has to be emphasised that hybrid warfare goes against the main purpose of the UN Charter of maintaining international peace and security. Even without an armed attack, hybrid warfare shakes international security by destabilising states, raising animosity and distrust in international relations.

Hybrid warfare exploits vulnerabilities of states and proves successful if nations have many weak spots. Ukraine is one of those states with vulnerabilities. The Ukrainian society is mainly susceptible to information war, owing to the wide mistrust towards

government, economic and political instability, and the common Soviet past with Russia, which makes it unthinkable for some that the brotherly nation can wage hybrid warfare. Therefore, the only way to be resilient to this hybrid threat is to fix current vulnerabilities within the country. This is a long-term process but the only solution.

Margarita Biryukova *holds a BA degree in International Affairs from John Cabot University (Rome, Italy) and LL.M. in European and International Law from Europa-Institut (Saarbrucken, Germany). She has worked in the OSCE Secretariat and the OSCE Special Monitoring Mission to Ukraine. Her main research interests include human rights, post-Soviet space, hybrid warfare, and Russia-Ukraine relations.*

Issue 3 (21), 2020
ISSN 2518-7481