

Larysa Kompantseva vol. 48, no. 1 (2021): 69-83 https://doi.org/10.11610/isij.4804

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Research, Education, and Practice of StratCom in the Security Service of Ukraine in Interagency Settings

Larysa Kompantseva 🕩

National Academy of the Security Service of Ukraine, Kyiv, Ukraine http://www.academy.ssu.gov.ua

ABSTRACT:

This article discusses how strategic communications (StratCom) were established in the security institutions of Ukraine's scientific and practical schools. An example of good practice is the approach of the National Academy of the Security Service of Ukraine, which was among the first in the security and defence sector of the state to become a platform for the formation of the scientific and practical school on StratCom. This process was carried out based on the following principles: building a "single voice" communication with security and government institutions, scientists, civil society representatives, journalists, and volunteers; establishing a scientific and practical discourse on strategic communications based on the concepts of "national values," "truth," "trust"; implementation of the "say-do" approach; promoting professional legal support and linguistic expertise of the information environment; focusing on practical results of scientific and educational activities; training of personnel in the field of strategic communications capable of working effectively at the strategic, operational and tactical levels. This approach aims to ensure the systematic implementation of strategic communications both at the institutional and the state levels.

ARTICLE INFO:

KEYWORDS:

RECEIVED: 28 MAR 2021
REVISED: 23 MAY 2021
ONLINE: 02 JUNE 2021

strategic communications, SSU, SSU Academy, security sector, defence sector, single voice communication, nationwide coordination, countering hybrid threats. StratCom coordination.



Creative Commons BY-NC 4.0

Introduction

The hybrid nature of modern conflicts has blurred the concepts of war, peace, and victory. Information technologies have changed the role of the average citizen in shaping the security discourse of the state. In parallel, the question of developing new tools for national security's geopolitical dimension enabling communication among security institutions of the world arose: "A person who has free access to information, and a new person has it from the moment of their birth, is different."

Therefore, ensuring national security starts with communications and building a communications strategy for different target audiences. This is the most recent challenge for institutions of security and defence sectors in Ukraine and all over the world. Strategic Communications (StratCom)—a new paradigm of cooperation and coordination of all actors involved in ensuring national and global security—are the answer to this challenge: "In today's information environment, the coordinated and timely use of the StratCom is important for achieving overall success, in particular in the context of hybrid warfare. ... strategic communications should be organised and implemented in such a way as to be effective in peacetime, a special period and during resolution of a conflict. The level of integration, simplicity and the speed of processes should be such that information and communication aspects are present at all levels of policymaking, planning and implementation, and are fully connected with other operational effects."²

The article presents the history and practice of the development of the Interdepartmental Interaction Platform "Strategic Communications in the Context of Hybrid Warfare" at the National Academy of the Security Service of Ukraine through the prism of forming a strategic communications system in Ukraine. This national experience demonstrates how, in crisis conditions at the horizontal level, it is possible to create an effective system of interagency interaction, to establish effective cooperation with foreign partners, to form a pool of scientists and practitioners working in different institutions, yet united by a common task — ensuring national security. The National Academy of the Security Service of Ukraine has been among the first to demonstrate the successful practice of inter-agency integration, due in large part to the conditions created for unification on its platform of representatives of the military and civilian sectors — members of scientific and educational institutions of Ukraine, volunteers, and journalists.

Ukraine's Experience in Interagency Cooperation in Defining a StratCom Policy

Ukraine was among the first states to introduce a strategic communications concept at the *state* level. Following the signing of the *NATO-Ukraine Road Map of the Partnership Program on Strategic Communications* ³ in 2015, the concept of strategic communications was enshrined in the *Military Doctrine of Ukraine* ⁴ and the *Doctrine of Information Security of Ukraine*.⁵

Ukraine equally was among the first countries to introduce a strategic communications concept at the *national* level.

The NATO-Ukraine Partnership in Strategic Communications was launched in 2015 at the official request of the National Security and Defence Council of Ukraine with the aim to seek support for the Ukrainian government in the field of strategic communications from NATO's Public Diplomacy Division. Among the overall objectives of the Partnership were (and still are) the following: to develop capabilities of Ukrainian authorities in the field of strategic communications and all its components at the strategic and operational levels by providing advisory and practical support; to support Ukraine's cooperation with experts having relevant experience in the field of strategic communications; to promote the development of a strategic communications culture at the institutional level in Ukraine; to support closer cooperation between non-governmental actors and to develop their ability to carry out strategic communications to the benefit of Ukraine; to achieve and maintain the highest standards of accuracy and ethics to ensure trust in the national communication policy.

The institutions involved in the Partnership are also defined in the Roadmap. On NATO's part, these are the NATO Public Diplomacy Division; a NATO Spokesperson; the International Military Staff (IMS) Public Affairs and StratCom Advisor (PASCAD); the Supreme Allied Commander Europe (SACEUR) Strategic Communications Division; the NATO Liaison Office (NLO) Ukraine; the NATO-Ukraine Training Program; the NATO Strategic Communications Centre of Excellence. On Ukraine's part, the Administrative Office of the NSDC, the Ministry of Defence of Ukraine, the Ministry of Foreign Affairs of Ukraine, and the Security Service of Ukraine (SSU) were confirmed as institutions providing strategic communications in Ukraine.

The intention of interagency cooperation and coordination is laid down in the definition of StratCom – "the coordinated use of communicative capabilities of the state – public diplomacy, public relations, military public communications, information and psychological operations, actions aimed at advancing the goals of the state." ⁶

Institutions and units tasked with taking up the issue of strategic communications began to develop gradually. For instance, during the 2015-2019 period, the *Ministry of Information Policy of Ukraine* was intended to function as the central government agency responsible for ensuring Ukraine's information sovereignty (in particular regarding dissemination of socially important information in Ukraine and abroad, as well as ensuring the functioning of national information resources).

This Ministry should have dealt with the inter-agency coordination of strategic communications but never did so satisfactorily.

The process of institutionalisation of strategic communications has been intensified in the meantime, and several units engaged in dealing with StratCom issues have been created:

- at the national level: the International Centre for Counter-Disinformation at the NSDC, the Centre for Strategic Communications and Information Security at the Ministry of Culture and Information Policy of Ukraine;
- in the security and defence sector: the Department of Strategic Communications and Public Relations of the Ministry of Defence of Ukraine, the Strategic Communications Department of the Commander-in-Chief of the Armed Forces of Ukraine; the Main Centre for Strategic Communications of the State Border Guard Service of Ukraine; the Department of Communications and Public Diplomacy of the Ministry of Foreign Affairs of Ukraine;
- at the level of educational and scientific units in military higher education institutions: the Department of Strategic Communications, Educational and Research Centre of Strategic Communications in the Sphere of National Security and Defence of the National Defence University of Ukraine; the Department of Philology, Translation Studies and Strategic Communications, National Academy of the National Guard of Ukraine;
- at the level of advisers/assistants to heads of security and government institutions on StratCom issues. Such positions have been introduced at the Office of the President of Ukraine, the State Border Guard Service of Ukraine, and the Ministry of Defence of Ukraine.

However, the inter-agency interaction and cooperation are still carried out mainly at the horizontal level and stem from the interaction among individual institutions, departments, and scientific schools.

The viability of StratCom, as is true for any new policy trend, relies upon its development and systematisation by scientific and practical schools.

Strategic Communications in Scientific Schools

The *scientific school* concept has received particular attention in the security and defence sector of Ukraine in recent years, but its required characteristics are not yet well established. Based on the author's experience, the requirements in security institutions should be as follows: the presence of a leader who not only sets the vectors of scientific research but also contributes to the formation of a pleiad of young scientists, who, with time, will "outgrow" their teacher and become prominent figures in science; continuity; advanced levels of research in a specific scientific field; intellectual and emotional unity; academic reputation and traditions; informality of communication. Interdisciplinarity and a systematic approach, which involve research "at the intersection" (the use of methodologies and approaches of different sciences, the involvement of specialists in different areas in the joint solution of a common task and, as a result, the development of a comprehensive research methodology and its implementation) should be the key parameters.

StratCom are a fairly new area of research and practice. Its development requires both scientific confidence and scientific openness.

The 'core' of StratCom is in coordinating communications, which is possible only if there is open interaction of specialists of various scientific specialties in various security institutions.

The activities of StratCom scientific schools mirror the situation of hybrid warfare: hybrid challenges and confrontations lead to the emergence of different methodologies, technologies, and practices. This is why we can observe today the dynamic formation of scientific schools in the field of StratCom of which some are following the vector of NATO and Ukraine, and others that of the Russian Federation – obviously with different intentions and results.

NATO's StratCom research centre is the NATO StratCom Centre of Excellence in Riga (NATO StratCom COE). In addition to studying all components of the StratCom, the Centre conducts scientific and practical research programs on clearly defined issues relevant to global security, i.e.: establishing communications with different target audiences in a post-truth situation;^{8,9,10,11} markers of manipulative communications;^{12,13} psycholinguistic dimensions of psychological and information operations in social networks;^{14,15,16} and countermeasure techniques to deep fakes.¹⁷ The indicators of the high communication standards of this school of thought are the following: the results of research and practical findings are published monthly on the website (https://www.stratcomcoe.org); the scientific journal "Defence Strategic Communications" ¹⁸ is published annually; the "Riga StratCom Dialogue" conference ¹⁹ gathering StratCom specialists from almost all over the world is held annually.

In the Russian Federation, the trend towards weaponised hostile StratCom is prevalent – all research fields which study communicative issues work within a single government program, the purpose of which is to develop communicative technologies of hybrid warfare. Thus, for instance, experts at the Siberian Federal University (Krasnoyarsk) claimed that introducing a new branch of linguistics was necessary, namely the linguistics of information and psychological warfare (O. Skovorodnikov, G. Kopnina, etc.).²⁰

Along similar lines in Yekaterinburg, the scientific school of the Institute of Philosophy and Law, Ural Branch of the Russian Academy of Sciences, works on the issue of the Russian version of "soft power" (O. Rusakova, E. Grybovod), ²¹ the school of Ural State Pedagogical University studies psycholinguistic features of discourses of influence (L. Vesnina, O. Nakhimova), ²² and the Superior School of Journalism and Mass Communication at St. Petersburg State University explores the psycholinguistic potential of media content as a tool of information and psychological operations (D. Havra, M. Labush, O. Sidorov). ²³

Ukrainian scientists of the security and defence sector have prioritised developing a proactive StratCom system capable of countering any hybrid challenges. Today, three StratCom scientific schools are leading in the security institutions. More specifically, professional communications in the strategic dimension are supervised by specialists of the National Academy of the National Guard of Ukraine (L. Pelepeychenko, I. Lysychkina);²⁴ the new scientific school of the National Defence University named after Ivan Chernyakhovskyi (O. Salnikov, T. Dzyuba)²⁵ established a training and research centre of StratCom in the field

of security and defenve. Since 2016, after the signing of the *Strategic Communications Partnership Roadmap* between the National Security and Defence Council and the NATO International Secretariat, ²⁶ the National Academy of the Security Service of Ukraine was among the first to become a platform for the formation of the StratCom scientific and practical school in the security and defence sector of the state.

StratCom at the National Academy of the Security Service of Ukraine: Research, Education, Training, and the Inter-departmental Interaction Platform "Strategic Communications in the Context of Hybrid Warfare"

Effective practice, as a rule, is based on effective methodology. Since in Ukraine StratCom is formed mainly on a horizontal level by the committed security and government institutions, an urgent need to create a single scientific and practical platform for coordination of inter-departmental interaction emerged. Such a platform named "Strategic Communications in the Context of Hybrid Warfare" was created at the National Academy of the Security Service of Ukraine. Its activities were/are aimed at (1) generalisation and analysis of the actual national experience in countering Russian aggression in the East of Ukraine; (2) development of the theory of StratCom as a scientific basis for ensuring the national security of Ukraine; (3) development of mechanisms for the use of StratCom to counter hybrid threats.

These three areas ensure the systematic implementation of StratCom both at the institutional and the state levels. "It is very difficult to counteract the Russian Army with its combat aircraft, missile weapons and nuclear arsenal in linear warfare. But no army is able to overcome the people who act in an organised and systematic way."²⁷

The development of the platform requires a unity of efforts; hence the formation of a research and practical school of StratCom was carried out according to the following principles:

- compliance with the provisions of the *Military Doctrine of Ukraine* ²⁸ and the *Doctrine of Information Security of Ukraine* ²⁹ regarding the adequate response of institutions of the security and defence sector of Ukraine to the challenges to national security and hybrid risks;
- building a "single voice" communication with security and government institutions, scientists, civil society representatives, journalists, and volunteers for ensuring Ukraine's national security;
- formation of a scientific and practical discourse of StratCom based on the concepts "national values," "truth," "trust";
- implementation of the "say-do" approach;
- ensuring professional legal and linguistic expertise of the information environment;
- focus on the practical results of scientific and educational activities;

 training of personnel in the field of StratCom, capable of working effectively at the strategic, operational, and tactical levels.

Several policy-relevant scientific inquiries were initiated regarding different segments of StratCom. The cooperation of specialists of various security and government institutions, journalists, bloggers, and volunteers resulted in the monographs "Formation and Development of the Strategic Communications System for the Security and Defence Sector of Ukraine,"³⁰ "Strategic communications in Hybrid War Environment: from Volunteer's View to Scientist's Opinion,"³¹ "Hybrid War: Suggestion and Counter-suggestion Technologies."³² These studies analyse and summarise the theoretical and conceptual comprehension of StratCom, propose methodologies and techniques of asymmetric response to hybrid aggression, and provide practical recommendations for specialists in governmental and security institutions on how to counter destructive hybrid influences based on the assessment of international and Ukrainian expertise in StratCom, i.e., the coordinated application of state communicative possibilities, namely public diplomacy, public relations, military relations, information and psychological means.

Academic research has been adapted for the educational process and supplemented with practical cases in textbooks such as "Internet-communication in the Activities of the Security Sector Institutions: Theoretical and Applied Aspects,"33" Social Communications for Experts of Security and Defence Sectors,"34" Research Methodology and Application of Internet-Resources (for Scientists in Defence and Security),"35" Linguistic Evaluation of Social Networks,"36 and practical guidelines "Strategic Communications for the Security and Defence Sector Specialists."37 These manuals highlight the practical use of StratCom in the day-to-day activities of experts of security and defence sectors, particularly in conditions of counter-terrorist operations and hybrid wars. Of particular value are the trainings, practical guidelines developed according to the subject area of each edition, and algorithms of communication actions in the framework of professional interactions.

The StratCom concept of Ukraine provides for a "360-degree view." It involves strategic thinking and philosophy, the understanding and evaluating the synergy of hybrid threats, the study of influence and target audiences, integration of politics, actions, words, etc. These tasks are discussed in the "Dictionary of Basic Concepts of Strategic Communications: Standards Based on NATO Documents (English-Ukrainian and Ukrainian-English)." The Dictionary generalises the standards proposed in NATO documents, which are in great demand today not only among experts in the security and defence sector institutions, but also among state and government agencies. The Dictionary was among the first dictionaries of basic concepts of StratCom prepared and published not only in Ukraine but also in the Euro-Atlantic security space at large.

The National Academy of the Security Service of Ukraine has traditionally been publishing specialised issues of the journal "Information Security of People, Community, State."³⁹ Issue no. 1 (2017) was devoted to the problems of StratCom. Its publication coincided with the approval by the President of

Ukraine of the *Doctrine on Information Security of Ukraine*. The authors of the journal are representatives of the security and defence institutions of Ukraine (the National Academy of the Security Service of Ukraine, the National Academy of the National Guard of Ukraine, the National Defence University of Ukraine named after Ivan Chernyakhovsky, the State Border Guard Service of Ukraine), leading research institutions (National Institute for Strategic Studies) and educational institutions (Taras Shevchenko National University of Kyiv), as well as military journalists, practical psychologists, volunteers. Such cooperation in the research sphere provides a basis for StratCom, based on the "efficient cooperation between government bodies and institutions of civil society in the time of formation and implementation of the government policy in the information sphere."⁴⁰ The journal issue thus supported the new paradigm of ensuring national security through StratCom.

Research on StratCom is further actively implemented in doctoral dissertations carried out by representatives of various security and state institutions at the premises of the National Academy of the Security Service of Ukraine.

Interdisciplinary and interagency approaches to StratCom are prevalent during the discussions which take place at the annual All-Ukrainian Scientific Conference of Young Scientists "Communication Strategies of the Information Society: Linguistics, Law, Information Security," which has been gathering representatives of both military and state educational institutions, leading StratCom researchers and practitioners for 12 years.

What is Taught and How: Courses (Trainings) for Experts of Public Authorities and the Security and Defence Sector of Ukraine in the Field of StratCom

The Academy offers training for various categories of security service employees in the field of StratCom, in particular in the following areas:

- detection of hostile StratCom and mechanisms for comprehensive assessment thereof, counteraction to their influence, and neutralisation;
- StratCom in the context of hybrid warfare;
- mechanisms for implementation of StratCom and interaction of security sector institutions and state authorities with media;
- StratCom and certain information campaigns: organisational and institutional features;
- StratCom in social networks: creation and distribution of content;
- methodology of StratCom in the media sphere, public relations, and public diplomacy;
- methodology of information and psychological operations in the StratCom system;
- communication technologies of leadership in the system of StratCom.

A number of trainings were conducted for representatives of other military and state institutions and foreign partners (See Table 1).

Table 1. Modules of Training Courses on Strategic Communications.

_	
Module	Content of the Module
Strategic Communications: Subject, Object, Basic Concepts, History of Development	Topical issues of StratCom between security and government institutions in the context of hybrid warfare. Constructive and destructive StratCom. Hybrid challenges and asymmetric counteraction. StratCom technologies in the event of a crisis. Principles and technologies of StratCom management during anti-terrorist activities. "Situational" StratCom of non-governmental organisations and government agencies
Destructive Strategic Communications in Russia's Hybrid Aggression	The concept of destructive StratCom. The legalisation of information aggression in the RF management documents. Practical implementation of the doctrinal provisions of the RF: information and psychological research in Ukraine and the world. Key narratives, genres, messages, technologies of the RF hybrid aggression. Proactive actions in conditions of a hybrid aggression
Organisational War as a Hybrid System	Multiformity of modern wars (informational, information-psychological, nonconventional, conscientious, systemic, organisational, etc.) as a developing paradigm of hybrid aggression. Organisational War: the essence, stages, and technologies. The peculiarities of using organisational weapons. Consciental operations. The system of organisational warfare in the paradigm of "Overtone Windows"
Legal Aspects of Strategic Communications in the Context of Hybrid Threats	Legal aspects of the international armed conflict in Ukraine. The correlation of international and national law in the field of protection of the peace against hybrid threats. Information operations as a component of crimes that infringe on national security and peace. Signs of hybrid nature of the crime of aggression in Ukraine and approaches to their legal assessment. Analysis of national judicial practice of legal assessment of crimes with components of hybrid threats. Detection and neutralisation of information technologies of influence which threaten the national security
Identification of Strategic Narratives	The narrative. The grand narrative. Strategic narrative. Strategic narrative in normative documents of Ukraine and NATO countries. Constructing a narrative. Key components of the narrative. The technology of creat-

	ing a narrative and deconstructing a hostile one. The development of a strategic Ukraine's narrative
Contra-suggestive technologies in the Conditions of Hybrid War	Hybrid war and system of values. Suggestion and contra-suggestion. Suggestive content of hybrid war: mythological design, media viruses, simulacra, speech markers of suggestive impact. Stages of suggestive programming to advance the hostile narrative. Contrasuggestive technologies. Contra-suggestive action practice
Strategic Communications in Social Networks	Philosophy and pragmatism of social networks. Mobilisation potential of social networks. Linguistic expertise of impact technology in social networks. Social networks recipients. Web-waves, media viruses, mems, and fakes as counter technologies. StratCom methodology in social networks
Strategic Communications in the Media Space	The Principles of Convergent Journalism. Practices of the interaction of security and state institutions with the media (technologies, genres, communicative behaviour). Interaction with the media in crisis conditions (preparation for the event, holding of the event, preparation and clarification of information). Answers to "inconvenient" questions
Strategic Communications in the Gender Dimension	Gender, conflict, communication. Conflict through gender lenses. "Gender" manipulative policy of the Russian Federation and countering it. Gender dimensions of peace and security in the StratCom system
Technologies of Information and Psychological Operations: the Ukrainian Experience	Information and psychological operations: different approaches. Stages of the RF information campaign against Ukraine. Priority information directions of the Russian Federation. The first active experience of 2014. The phase of "imposing peace." Possible scenarios of RF information aggression, preparation of asymmetric responses
Psychology of Strategic Communications	Psychological analysis of information and communications. System thinking, systemic aggression, systemic countering. Analysis of target audiences and psychological principles of interaction with them. Psychological deployment of StratCom
Information Operations Planning	Reasons for information operations planning. Formation of the planning group. Planning of information operations according to NATO standards: initiation

	phase, operation analysis, operation concept development, operation plan development, plan review (if necessary). Criteria for assessing the effectiveness of the operation
Leadership in Strategic Communications	Leadership in StratCom in the context of hybrid war- fare. The role of the leader in making the staff more active and involving them in achieving goals. Team- building in the system of StratCom. The leader's per- sonal image management techniques. Charisma as the ability to influence people
Presentation and Position- ing in the Organisation of Strategic Communications	Visualisation of communications. Design of speeches and presentations. The art of presentation in the security and defence sector

Training is carried out according to a modular system: based on the professional needs of the target audience, as well as on the level of previous training (tactical, operational, or strategic), a certain number of modules are selected for each training course. The overwhelming number of study sessions (about 90 %) is held in the format of trainings.

The distinguishing characteristic of the courses and their fundamental difference from similar initiatives in other state institutions are: the utilisation during training of integrated practical expertise of Ukraine in countering aggression in the East of Ukraine; carrying out targeted training; trainings are conducted with the participation of the best subject-matter specialists from government bodies, agencies of the security and defence sector, institutions of higher education and scientific institutes of Ukraine, representatives of civil society and volunteer organisations with practical expertise in the field of countering asymmetric challenges.

Today, about 30 instructors take part in the courses, including representatives of the Verkhovna Rada of Ukraine, leaders, and personnel of operational units of the Security Service of Ukraine, the State Border Guard Service of Ukraine, the Institute for National Strategic Studies, Taras Shevchenko National University of Kyiv, the Diplomatic Academy of Ukraine named after Hennadiy Udovenko at the Ministry of Foreign Affairs of Ukraine, the National Academy of the Public Prosecutor's Office of Ukraine, The National Writers' Union of Ukraine, Women's Information Consultative Centre, as well as media representatives, bloggers, volunteers, independent experts, etc.

The task of the courses is not only to teach trainees the methodology of Strat-Com but also to establish communication and interaction of security and government institutions with civil society for the long run.

Conclusions and Recommendations

The introduction of StratCom into scientific and educational activities of the National Academy of the Security Service of Ukraine involves, above all, the training of specialists of a new breed who are able to proactively counter any type of national security challenges. To achieve this, the Scientific and Practical School for Strategic Communications of the Academy worked consistently to fulfil the following tasks: to improve the system of training of the Security Service of Ukraine experts on StratCom, which is carried out at the premises of the National Academy of the Security Service of Ukraine, by launching such training for employees of public authorities and institutions of the security and defence sector of Ukraine; to create of a pool of scientists and experts whose main task is to develop modern methodologies and technologies for countering hybrid threats, in particular in the field of StratCom; to provide scientific substantiation of the concept of StratCom and to create a theoretical basis for the construction of the state system of StratCom in Ukraine; to develop and publish educational and scientific resources for the process of training of experts in StratCom.

This activity serves as an example of the institutional "open door policy," a step towards forming "single voice" communications. Due to interagency cooperation and interaction with civil society representatives, the Academy has created a platform for coordinating scientific and practical activities in StratCom of security and state institutions.

The experience gained, the achievements and mistakes, allowed me to formulate the following recommendations for institutions that are on their way to adopt the practice of StratCom:

- 1. It is necessary to form a long-term strategy for implementing StratCom in the institutions; to determine tactical and operational tasks.
- 2. It is essential to adopt a systemic approach to the implementation of Strat-Com. This means finding reliable partners among other security and government institutions and civil society, identifying points of contact (institutional values, challenges, trends, etc.), and using them in a bid to promote StratCom.
- 3. Practice is blind without theory. Therefore, for the StratCom system to work, the coordination and interaction of various actors, such as experts of security and state institutions, scientists, journalists, and volunteers, is essential.
- 4. The policy of prioritizing own interests flaws the implementation of Strat-Com. There can be no predetermined or privileged "main" science or institution. Instead, the leader is the one who offers an effective methodology and practical expertise at the intersection of sciences and interagency interests.
- 5. It is necessary to determine a national system of values, in particular to define national and institutional narratives and messages; to provide them based on information sources focusing on different target audiences; and to offer their scientific justification.
- 6. The theory of StratCom must proactively ensure effective asymmetric practices of countering hybrid threats.

Research, Education and Practice of StratCom in the Security Service of Ukraine

7. Training of StratCom specialists is possible only when the (best available) experts, i.e., the representatives of security and state institutions, scientists, journalists, bloggers, and others, are engaged.

References

- Georgij Pocheptsov, "The Management of State Affairs Rests with Communications, not with Truncheons," *Rezonans*, 2020, https://rezonans.kz/upravlenie-gosudarstvom-chast-1.
- "NATO Military Policy on Strategic Communications," MC 0628, Supreme Headquarters Allied Powers Europe, 2017, http://stratcom.nuou.org.ua/wp-content/uploads/2020/01/NATO-MILITARY-POLICY-ON-STRATEGIC-COMMUNICATIONS.pdf.
- "A Roadmap of the Partnership Program on Strategic Communications between the National Security and Defence Council and NATO International Staff," Ukraine-NATO, 2015, https://ukraine-nato.mfa.gov.ua/dokumenti/dokumenti-dvostoronnogospivrobitnictva. – in Ukrainian.
- ⁴ "The Military Doctrine of Ukraine," approved by Presidential Decree no. 555/2015, https://www.president.gov.ua/documents/5552015-19443.
- Decree of the President of Ukraine no. 47/2017, "On the National Security and Defence Council of Ukraine Decision of 29.12.2016 'On the Doctrine of Information Security of Ukraine,'" https://www.president.gov.ua/documents/472017-21374.
- 6 "The Military Doctrine of Ukraine".
- ⁷ Larysa Kompantseva, "Strategic Communications in the Dimension of Scientific Schools," First International Scientific and Practical Conference "Strategic Communications in the Sphere of Ensuring National Security and Defence: Problems, Experience, Perspectives" (Kyiv: Ministry of Defence of Ukraine, the National Defence University named after Ivan Chernyakhovskyi, 2020): 100-102.
- Francesca Granelli, "What Does It Mean for a Communication to be Trusted?" Defence Strategic Communications 5 (2018): 171-214, https://doi.org/10.30966/ 2018.RIGA.5.5.
- ⁹ Karen Allen, "Communicating Threat in an Era of Speed and Fetishised Technology," Defence Strategic Communications 8 (2020): 203-215, https://doi.org/10.30966/ 2018.RIGA.8.7.
- Rueban Manokara and Marina Paramonova, Manipulation Ecosystem of Social Messaging Platforms (Riga: NATO Strategic Communications Centre of Excellence, 2020), https://www.stratcomcoe.org/messaging_manipulation_services_web_7mai.pdf.
- Sebastian Bay and Rolf Fredheim, Falling Behind: How Social Media Companies are Failing to Combat Inauthentic Behaviour Online (Riga: NATO Strategic Communications Centre of Excellence, 2019), https://www.stratcomcoe.org/how-social-mediacompanies-are-failing-combat-inauthentic-behaviour-online.
- Hannah Smith, Online Influence and Hostile Narratives in Eastern Asia (Riga: NATO Strategic Communications CoE, 2020), https://www.stratcomcoe.org/online-influence-and-hostile-narratives-eastern-asia; Manokara and Paramonova, Manipulation Ecosystem of Social Messaging Platforms.
- Andrew Park, Matteo Montecchi, Mitsu Cai Feng, Kirk Plangger, and Leyland Pitt, "Understanding 'Fake News': A Bibliographic Perspective," *Defence Strategic Communications* 8 (2020): 141-172, https://doi.org/10.30966/2018.RIGA.8.4.

- Sebastian Bay, Anton Dek, Iryna Dek, and Rolf Fredheim, Social Media Manipulation 2020. How Social Media Companies are Failing to Combat Inauthentic Behaviour Online (Riga: NATO Strategic Communications Centre of Excellence, 2020), https://www.stratcomcoe.org/social-media-manipulation-report-2020.
- Berfin Kandemir and Alexander Brand, Social Media in Operations a Counter-Terrorism Perspective (Riga: NATO Strategic Communications Centre of Excellence, 2017), https://www.stratcomcoe.org/social-media-operations-counter-terrorismperspective.
- Jente Althuis and Leonie Haiden, eds., Fake News: A Roadmap (Riga: NATO Strategic Communications CoE, 2018), https://stratcomcoe.org/publications/fake-news-a-roadmap/137.
- ¹⁷ Rolf Fredheim and Kristina Van Sant, *Robotrolling*, quarterly bulletin, issues 2, 3 & 4 (2020), https://stratcomcoe.org/search?q=robotrolling.
- ¹⁸ Defence Strategic Communications, https://stratcomcoe.org/projects/academic-journal.
- ¹⁹ Riga StratCom Dialogue, https://rigastratcomdialogue.org.
- ²⁰ Aleksandr Skovorodnikov, ed., *Linguistics of Information-Psychological Warfare* (Krasnoiarsk: Siberian Federal University, 2017), Book I and Book II.
- Olga Rusakova, ed., Soft Power: Theory, Resources Discourse (Yekaterinburg: Publishing House "DISCURS-P," 2015).
- Liudmila Vesnina and Elena Nakhimova, "Information-Psychological Wars in Russia," Political Linguistics 3 no. 63 (2017): 140-145.
- The Information Century (St. Petersburg: St. Petersburg State University, 2014-2021), http://jf.spbu.ru/about/825.html; Viktor Sidorov, ed., Communicative Aggressions of the 21st Century (St. Petersburg: Aleteyya, 2019); Nikolai Labush and Anatolii Puiu, Mediatisation of Extreme Forms of Political Process: War, Revolution, Terrorism (St. Petersburg: St. Petersburg State University, 2019).
- Liudmyla Pelepeichenko, Theoretical and Practical of Strategic Communications of the National Guard of Ukraine (Kharkiv: National Academy of the National Guard of Ukraine, 2017).
- ²⁵ Official Website of the Educational and Research Centre of Strategic Communications in the Sphere of National Security and Defence of the National Defence University named after Ivan Chernyakhovskyi, http://stratcom.nuou.org.ua.
- Educational and Research activities in the NA SSU in the sphere of Strategic Communications started pursuing Clauses 6, 7 of the Action Plan on the Road Map of Partnership Program on Strategic Communications between National Security and Defence Council and NATO International Staff (approved by the Secretary of NSDCU on 05.11.2015), Clauses 4, 5 of the SSU Implementation Plan on the Road Map of Partnership Program on Strategic Communications between National Security and Defence Council and NATO International Staff (approved by the Head of the Security Service of Ukraine on 30.12.2015).
- ²⁷ Volodymyr Horbulin, *How to Defeat Russia in the Wars of the Future* (Kyiv: Bright Books, 2020).
- ²⁸ "The Military Doctrine of Ukraine."
- ²⁹ Decree of the President of Ukraine no. 47/2017.

Research, Education and Practice of StratCom in the Security Service of Ukraine

- Volodimir Pylypchuk, Larysa Kompantseva, Sergiy Kudinov, and Oleksandr Zaruba, Formation and Development of the Strategic Communications System for the Security and Defence Sector of Ukraine (Kyiv: Ltd ArtEk Publishing House, 2018).
- ³¹ Larysa Kompantseva, ed., *Strategic Communications in Hybrid War Environment:* from Volunteer's View do Scientist's Opinion (Kyiv: National Academy of the Security Service of Ukraine, 2018).
- ³² Larysa Kompantseva, Zaruba Oleksandr, Nataliya Slukhai, and Olena Snitko, *Hybrid War: Suggestion and Counter-Suggestion Technologies* (Kyiv: National Academy of the Security Service of Ukraine, 2018).
- ³³ Larysa Kompantseva, ed., *Internet-Communication in the Activities of the Security Sector Institutions: Theoretical and Applied Aspects: Monograph* (Kyiv, Luhansk: Yantar, 2013).
- Larysa Kompantseva, Social Communications for Experts of Security and Defence Sectors: Manual (Kyiv: National Academy of the Security Service of Ukraine, 2016).
- ³⁵ Larysa Kompantseva, ed., *Research Methodology and Application of Internet-Resources (for Scientists in the Defence and Security Sector): Manual* (Kyiv: National Academy of the Security Service of Ukraine, 2014).
- ³⁶ Larysa Kompantseva, *Linguistic Evaluation of Social Networks: Manual* (Kyiv: National Academy of the Security Service of Ukraine, 2018).
- ³⁷ Larysa Kompantseva, ed., Strategic Communications for the Security and Defence Sector Specialists: Practical Guidelines (Kyiv: National Academy of the Security Service of Ukraine, 2018).
- ³⁸ Larysa Kompantseva, ed., *Basic Concepts of Strategic Communications: Standards Based on NATO Documents (English-Ukrainian and Ukrainian-English)* (Kyiv: National Academy of the Security Service of Ukraine, 2019).
- ³⁹ Information Security of People, Community, State: Journal no. 1 (2017).
- ⁴⁰ Decree of the President of Ukraine no. 47/2017.

About the Author

Larysa F. **Kompantseva**, Doctor of Philology, Professor, Head of the Department of Theory and Practice of Translation at the National Academy of Security Service of Ukraine (Kyiv, Ukraine), is one of the founders of scientific schools on Internet Linguistics and StratCom in Ukraine. Recently she has been involved in research programs on the linguistic expertise of social networks using Big Data tools, and the communication sphere as a component of national security. https://orcid.org/0000-0001-7902-9209