Countermeasures for Hybrid Threats: The Experience of the European Union and Its Member States

D. Yu. Bazarkina*

Institute of Europe (IE), Russian Academy of Sciences, Moscow, Russia
e-mail: bazarkina-icspsc@yandex.ru

Received October 24, 2021; revised January 22, 2022; accepted January 27, 2022

Abstract—The methods and tools used by the European Union to counter hybrid threats are identified: from the fight against terrorism to measures aimed at combating economic competitors and political opponents (mainly, to squeeze Russia and China out of European markets). It is concluded that it is not by chance that neither EU institutions nor the research community have worked out a comprehensive definition of operations to combat hybrid threats. A broad understanding of hybrid threats as practically any (depending on the political situation) actions of the opponent serves to justify the application of any counteraction tool. In the fight against global threats such as terrorism, cybercrime, and the spread of false medical data, the EU takes a systemic approach, which makes it possible to assess the level and degree of the convergence of threats to critical infrastructure and the infosphere, as well as the possibilities of counteraction. At the same time, attempts to use economic, legislative, political, and informational tools to achieve one-sided economic, political, and military advantages do not reduce the degree of tension in the EU’s relations with Russia, China, and some other countries, only increasing the number and strength of hybrid threats. This reduces the EU’s ability to achieve strategic autonomy.

Keywords: hybrid operations, hybrid campaigns, hybrid threats, European Union, European Commission, European Parliament, European Union External Action Service

DOI: 10.1134/S1019331622100033

Against the backdrop of growing international tension and accusations against state actors of creating hybrid threats for other countries or integration associations, it is topical to analyze the practice of combating hybrid threats in national and supranational structures. The purpose of this article is to identify the methods and tools through which the practice of countering hybrid threats is being implemented in the EU, both with positive goals (such as combating cybercrime) and as part of the ousting of economic competitors (mainly Russia and China) from European markets and political opponents from the infosphere. Achieving this purpose requires answering the following research questions: (1) How are operations to counter hybrid threats defined? (2) How do the EU and its member states carry out operations to combat hybrid threats relevant to third countries, including Russia (in particular, regarding actions of terrorist organizations, cybercrime, etc.)? (3) How does the EU use the approach to countering hybrid threats to explain the measures taken against economic competitors and political opponents (especially in the context of US–China trade wars and US and EU tensions with Russia)?

HYBRID THREATS, HYBRID CAMPAIGNS, AND HYBRID THREAT COUNTERMEASURES: DESIGNATION ISSUES

Both in theoretical works and in official EU documents, the concepts of hybrid operations and hybrid campaigns are very closely related to the concept of hybrid threats. The line between them is often vague. Thus, F. Hoffman, whose works underlie the theory of hybrid warfare, in works of different years gives almost identical definitions of hybrid warfare [Hoffman, 2007, p. 29] and threats [Hoffman, 2010, p. 444], highlighting the combination of conventional weapons, irregular tactics, terrorism, and criminal behavior on the battlefield. Most likely, this was one of the causes of a certain confusion about the concepts of war and threat both in subsequent scientific publications and in strategic documents, including in the EU. Nevertheless, while Hoffman focuses primarily on the conduct of war (including by nontraditional means), in the later definitions by EU and NATO experts, the concept of hybrid threats is gradually changing (for

* Dar’ya Yur’evna Bazarkina, Dr. Sci. (Polit.), is a Leading Researcher in the RAS IE Department of European Integration Research.
example, such threats are interpreted as widespread use of traditional and nontraditional means by the enemy to achieve their goals).

The European External Action Service (EEAS) characterizes hybrid threats primarily as actions, listing their options from cyberattacks to disruption of energy supplies. While the understanding of a threat as, for example, a state capable of developing into a military conflict (such an interpretation is present in the Military Doctrine of the Russian Federation) implies the absence of this conflict and is not always associated with a subjective factor (the enemy) alone, a threat as an action always implies active efforts of the enemy, which in this situation ceases to be a suspected one; consequently, countermeasures will be aimed not so much at resolving the situation as at limiting the capabilities of the other side. A stable definition of operations to counter hybrid threats has not yet been developed either; rather, it is formulated from the contrary (the fight against disinformation, cybercrime, foreign interference, etc.). All this makes it difficult to analyze theoretically the fight against hybrid threats, especially when the combination of traditional and nontraditional actions has become a feature of the very system of international relations [Cusumano and Corbe, 2018, p. 6]. Note, however, that in relation to actors such as criminal and terrorist organizations, the assessment of any action as a threat is quite fair due to their inherently antisocial nature.

The term hybrid campaign, which has not yet fully taken shape in the scientific literature, is equally difficult to define. The components of a hybrid campaign are information operations (which justifies the use of counterpropaganda as a response), cyberattacks, espionage, actions of proxy structures (for example, people or organizations that are conductors of the enemy’s propaganda), and economic and political influence and pressure [Mareš, Holzer, and Šmíd, 2020, pp. 39–41]. Both in theoretical works and in the EU’s approach, certain double standards can be traced: hybrid campaigns, actions, or operations are always those of the enemy, while “countering hybrid threats” is the prerogative of the “goodie” [this is noted by Simons, 2021; Fridman, 2018], identifying as the defensive side.

At the same time, the broad interpretation of hybrid threats adopted in the EU serves as a solid justification for initiatives to develop space infrastructure, health care, food security, etc., as branches of ensuring the security of society. Hence, measures to counter hybrid threats are understood as programs to protect critical infrastructure, health, etc. Operations against hybrid threats in such areas imply, for example, the fight against sabotage in food production or misinformation discrediting scientific approaches in medicine; i.e., they provide an objective benefit. Such operations begin to acquire a negative tenor when they are aimed at squeezing out an economic competitor, limiting the opponent’s freedom of speech in the information space, and expanding military blocs.

POSITIVE EXPERIENCE OF COUNTERING HYBRID THREATS IN THE EU

The experience of the EU in combating hybrid threats is considered using examples from only a few areas (prevention of terrorism, suppression of propaganda, cybercrime, and disinformation related to the coronavirus infection pandemic). Since mid-2020, these threats have increased around the world, and there are predictions artificial intelligence will increasingly be used for criminal purposes [Caldwell, Andrews, Tanay, and Griffin, 2020]. The pandemic and the associated crisis are being used by extremists and terrorists to spread their ideas. At the EU level, a number of agencies are responsible for countering the above threats, including the EU agencies for cooperation in the field of law enforcement (Europol), criminal justice cooperation (Eurojust), and the EU cybersecurity agency (ENISA).

A systematic approach to countering hybrid threats is being implemented in such key areas as the modernization and harmonization of legislation, the blocking of funding channels for the actors of hybrid threats, and the cooperation of supranational EU structures with national authorities (not only of the member states but also of third countries) within the framework of special operations. Technical security solutions are often provided by their developers, private companies. The unquestionable advantage of the system for combating hybrid threats in the EU is the reliance on expert knowledge, for which cooperation is established with as many specialists as possible, not only from security structures but also from the civil sphere, which makes it possible to assess the consequences of the measures taken for different groups and layers of society.

A useful example of coordinating the operational work of law enforcement officers of the EU, its member states, and third countries is EMPACT (European...
Multidisciplinary Platform for Combating Crime), which brings together specialists from law enforcement and judicial bodies, EU agencies, customs and tax services, and private companies. Europol reports are used within EMPACT by the Commission and President of the Council of the EU to advise Ministers of Justice and Home Affairs, who take the EU’s priorities in the fight against crime for four years as the basis of national operational action plans. EU and national-state coordinators organize joint police operations, which usually last several days or weeks. The EMPACT platform has shown its effectiveness, particularly in the fight against cybercrime, including the detention of twelve suspects in cyberattacks against critical infrastructure on October 26, 2021. The operation was attended by officers from Britain, Germany, the Netherlands, Norway, the United States, Ukraine, France, and Switzerland, which shows the high possibilities for coordinating such work by EU agencies, including those outside it.

Expert networks remain an important tool in the fight against the described group of hybrid threats, in particular, the Radicalization Awareness Network (RAN), created by the EU Commission in 2011 and uniting 6000 practitioners in the member states, working with groups at risk of terrorist recruitment, as well as with active sympathizers of terrorists and extremists. Network members share positive experiences, particularly in working with young people or using new ICTs. For example, the “Gaming with the Police” project, launched in the Netherlands in 2020, connects police officers with young people from risk groups in online games; 8 at present, this practice is used by 21 police teams in the country. The Belgian Federal Police shares its practice of interviewing children returned from conflict zones in the Middle East using a special protocol adapted to work with children. Steps are being taken to disseminate this experience not only through the RAN channels but also on the UN sites.

The cooperation between law enforcement and digital service providers helps create important practi-

5 Eurojust, 2021. EMPACT leaflet. https://www.eurojust.europa.eu/empact-leaflet. Cited December 7, 2021.
6 Europol, 2021. 12 targeted for involvement in ransomware attacks against critical infrastructure. https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure. Cited December 7, 2021.
7 European Commission, 2021. Radicalisation Awareness Network (RAN). https://ec.europa.eu/home-affairs/networks/radicalisation-awareness-network-ran_en. Cited December 7, 2021.
8 European Commission, 2021. Gaming with the police. https://ec.europa.eu/home-affairs/networks/radicalisation-awareness-network-ran-collection-inspiring-practices/ran-practices/gaming-police_en. Cited December 7, 2021.
9 European Commission, 2021. Interviews of returnee children. https://ec.europa.eu/home-affairs/networks/radicalisation-awareness-network-ran-collection-inspiring-practices/ran-practices/interviews-returnee-children_en. Cited December 7, 2021.
10 Europol and Eurojust view the project as an important step in formalizing cooperation between law enforcement and private companies, although its activity is still largely dependent on the goodwill of the latter. The adoption of the Digital Services Act, designed to strengthen the control of online platforms by EU institutions, will accelerate the introduction of mandatory assistance from digital service providers to law enforcement agencies.

Combating hybrid threats means not only stopping the activities of criminal actors but also conducting information campaigns to prepare society for protection against a growing threat or minimizing information and psychological damage from the actions of intruders. The participants in such campaigns are representatives of supranational EU institutions, national governments, media, business, and civil society institutions. Prevalent is the participation of EU agencies in information operations, among which is the Europol-initiated termination of the activities of 21 websites of groups affiliated with Al-Qaeda and the Islamic State, banned in Russia, in October 2021. The removal of content by Europol remains the main method of countering terrorist propaganda on the Internet. It receives more attention at the official level than, for example, the dissemination of counternarratives, developed primarily by representatives of civil society, or the redirection of search engine users to sites exposing terrorism (a method used by online platforms). In curbing pandemic-related disinformation, the EU is also relying on cooperation with major online platforms, for which the signing of the Code of Practice on Disinformation has made this work mandatory. In this area, tools to monitor and rank materials using artificial intelligence, the dissemination of counternarratives through the joint efforts of online platforms, governments, and the media are used.

11 Europol, 2021. 3rd Annual SIRIUS EU Digital Evidence Situation Report. European Union Agency for Law Enforcement Cooperation, The Hague, Netherlands, p. 9.
12 European Commission, 2021. Reports on June Actions—Fighting COVID-19 Disinformation Monitoring Programme. https://digital-strategy.ec.europa.eu/en/library/reports-june-actions-fighting-covid-19-disinformation-monitoring-programme. Cited December 7, 2021.
Of course, the agencies also discuss issues of foreign interference in EU affairs, which are currently deeply politicized. Europol refers to the EBU, repeating that state actors are spreading disinformation in an effort to destabilize governance in the European Union, but the department’s official website does not mention the specific practice of combating foreign interference. More attention is paid to this area by ENISA, the reports of which provide data on state-sponsored cyberthreat subjects; however, security practitioners generally avoid overly politicized assessments (including in the publications analyzed above).

HYPERPOLITICIZATION OF COUNTERING HYBRID THREATS

In the practice of countering foreign interference in EU affairs, excessive politicization is clearly manifested, including in economic issues. The clash of business interests and fierce competition are fundamentally inherent in capitalism. However, political elites are now increasingly involved in economic rivalry in the exchange of accusations of hybrid threats. This ultimately affects the quality of life and information and psychological security of citizens. In the process of squeezing Chinese and Russian companies out of the European market under the slogans of combating hybrid threats, one can trace both the economic interest of local and American suppliers and the political interest of the “Atlantists” as part of the European elite (which reduces not only the quality of EU international cooperation but also the ability of European US allies to strengthen real strategic autonomy [Danilov, 2021, p. 19]). Estonia, Latvia, and Lithuania are considered by the Atlantists as the primary object of Russian hybrid influence, which “is due to the continued energy dependence of these countries on Moscow” [Smirnov, 2020, p. 15].

The restriction of foreign influence is being undertaken in the EU using a scheme reminiscent of the set of measures to combat criminal actors, but with a number of differences. Thus, direct legislative bans on the activities of organizations from an opponent country (denied at the official level) can be replaced by bureaucratic obstacles (many stages of contract consideration, risks of vetoing, etc.) and sanctions pressure (even though it reduces the possibility of making weighted solutions [Bisop, 2021, p. 2] beneficial to both parties). Informational and psychological influence on citizens to discredit the opponent is being exerted, just like in the fight against terrorist propaganda, through all possible channels. Public state-

13Europol, 2020. Catching the virus cybercrime, disinformation and the COVID-19 pandemic. https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf. Cited December 7, 2021.
14ENISA, 2021. ENISA Threat Landscape 2021, European Union Agency for Cybersecurity (ENISA), Attiki, Greece, pp. 16–23.
15Regeringskansliet, 2021. “France and Sweden to further develop defence cooperation.” https://www.government.se/opinion-pieces/2021/09/france-and-sweden-to-further-develop-defence-cooperation/. Cited December 7, 2021.
16Spionageabwehr, 2021. Chinas neue Wege der Spionage. Single Point of Contact—SPOC. [online]. 1, pp. 30–34. https://www.verfassungsschutz.de/SharedDocs/Publikationen/DE/2021/spoc-wirtschaft-und-wissenschaft-schuetzen.html. Cited December 7, 2021.
17Huang C., 2021. International opinion of Russia and Putin remains negative in 2020. https://pewrs.ch/3888Nc1. Cited December 7, 2021.
Chinese telecommunications company Huawei from the EU countries. At the EU level, the Toolbox and the Report on risk assessment of 5G networks security indicate the possible interference of third countries in EU affairs if the 5G supplier has strong ties with the government of the country of origin or if the government can put pressure on the supplier in any form. The latter has been the subject of controversy since practically no company is completely free from the influence of the government of its home country. In the case of China, the reason for noncooperation in the EU countries is the National Intelligence Law, according to which Chinese companies must cooperate with the national intelligence service. A number of EU countries have already banned the use of Chinese 5G equipment; an example is Sweden, where telecom operators must exclude it from their infrastructure until 2025.

In Belgium, a scandal involving Huawei erupted in December 2020. The company sponsored an article by lawyer E. Vermulst criticizing the protectionist law on security measures for the implementation of 5G, which was forcing Chinese manufacturers out of the Belgian market. Later, this article, as well as several others, were circulated on Twitter using 14 fake accounts (according to the New York–based online disinformation investigation agency Graphika, their profile pictures were generated using artificial intelligence). Huawei representatives retweeted messages from fake accounts: according to Graphika, Kevin Liu (Huawei’s head of communications in Western Europe) made 60 such retweets within three weeks, and the official Huawei Europe account, 47. The agency admitted that it was impossible to establish who stood behind the incident. Of course, the mere fact that Huawei managers reposted tweets of fake profiles was a rash move. However, despite the uncertainty of the situation, several Belgian civil servants publicly accused Huawei of attacking the government’s reputation. Thus, the information was introduced into the already prepared infosphere, where the actions of companies from China are used to discredit the country.

Both the media of the EU countries and its government structures provide a platform for politicians who demand further pressure on Russia and Belarus. Certain double standards in the fight against hybrid threats are evidenced by S. Tikhanovskaya’s speech from the rostrum of the European Parliament; Tikhanovskaya de facto openly called for the undermining of public trust (one of the hybrid actions of which the EBU accuses potential opponents) in the Belarusian president, stating the need for the EU to use a “non-traditional” approach by reaching out to Belarusian civil society on the ground, in particular, by initiating the nonrecognition of the Belarusian authorities.

On November 28, 2021, during the visit of NATO Secretary General J. Stoltenberg to Latvia and Lithuania, President of the EU Commission U. von der Leyen called for closer cooperation between the EU and NATO in the fight against hybrid attacks. During this meeting, Director of the Joint EU—NATO Center of Excellence for Countering Hybrid Threats T. Tiilikainen accused Russia, China, and Iran of using nontraditional hybrid methods to compensate for the lack of influence at the international level, and the Belarusian government, of deliberately organizing a migration crisis. Attempts to connect the latter with the movements of the Russian military against the backdrop of accusations against Russia of plans to invade Ukraine are not new in the context of reports about the instrumentalization of migration on the Russian side (for example, in 2015 a number of such publications appeared in the Finnish media [Alenius, 2021]). There is reason to believe that in the EU, in a situation where “interests in the field of migration policy at different levels of government do not always coincide, and conflicts arise” [Potemkina, 2020, p. 109], blaming, first of all, external actors (Belarus and Russia) is used by the part of the European elite that seeks further confrontation.

**CONCLUSIONS**

Both in EU institutions and in the research community, there is no succinct definition of operations to combat hybrid threats. At the same time, the understanding of hybrid threats as practically any (depending on the political situation) actions of the opponent serves as a justification for applying countermeasures to the latter.

In the fight against global threats such as terrorism, cybercrime, and the spread of false medical data, the EU takes a systematic approach, where practice is constantly supported by expert knowledge. This makes it possible not only to assess the level and degree of convergence of threats to critical infrastructure and the infosphere, as well as the ability to counter them,
but also to develop tactics to combat them constantly, using the latest technical means and mastering the most relevant platforms (evidence of this is the development of a system of electronic evidence, improving the removal of extremist content, monitoring and suppressing cybercrime, and working with young people in their comfort zones, such as online games, etc.). As such initiatives develop, the fight against hybrid threats could become the basis of EU strategic communication as a synchronization of long-term policy and its communication support for internal and external audiences.

At the same time, in politically sensitive issues, such as the fight against foreign interference, a developed system for combating hybrid threats, combining economic, legislative, and political tools with information campaigns, is used in the framework of trade wars and related informational and psychological confrontation. This does not reduce the degree of tension in the EU’s relations with Russia, China, and some other countries, increasing the number and strength of hybrid threats, which can lead to a military threat and reduce the EU’s ability to achieve strategic autonomy.

CONFLICT OF INTEREST

The author declares that she has no conflicts of interest.

OPEN ACCESS

This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/.

REFERENCES

Alenius K. (2021) Asylum Seekers from Russia to Finland: A Hybrid Operation by Chance? in: Eze Th., Speakman L., Onwubiko S. (eds.) Proceeding of the 20th European Conference on Cyber Warfare and Security, ECCWS 2021, pp. 11–17, Academic Conferences International Limited, Reading, UK. https://doi.org/10.34190/EWS.21.069

Biscop S. (2021) The EU and China: Sanctions, Signals, and Interests. Security Policy Brief No. 145, May. EGMONT—Royal Institute for International Relations, Brussels, Belgium. URL: https://www.egmontinstitute.be/content/uploads/2021/05/SPB145-revised.pdf?type=pdf (accessed: 07.12.2021).

BAZARKINA

Caldwell M., Andrews J., Tanay T., and Griffin L. (2020) AI-enabled future crime. Crime Science, Vol. 9(1). https://doi.org/10.1186/s40163-020-00123-8

Cusumano E. and Corbe M. (2018) Introduction, in: Cusumano E. and Corbe M. (eds.), A Civil–Military Response to Hybrid Threats, Palgrave Macmillan, Cham, Switzerland. https://doi.org/10.1007/978-3-319-60798-6_1

Danilov D.A. (2021) Global’nye gorizonty atlanticheskogo alf’yansa: “vakcina” Bajdena. [Global Horizons of the Atlantic Alliance: the Biden “Vaccine”], Sovremennaya Evropa, No. 5, pp. 19–31, (In Russian). https://doi.org/10.15211/soveurope520211931

Fridman O. (2018) Russian ‘Hybrid Warfare’: Resurgence and Politicisation. Oxford University Press, New York, USA.

Hoffman F. (2007) Conflict in the 21-st century. The rise of hybrid wars, Potomac Institute for Policy Studies, Arlington, USA.

Hoffman F. (2010) ‘Hybrid Threats’: Neither Omnipotent Nor Unbeatable, Orbis, vol. 54, No. 3, pp. 441–455. https://doi.org/10.1016/j.orbis.2010.04.009

Mareš M., Holzer J. and Šmíd T. (2020) The Hybrid Campaign Concept and Contemporary Czech–Russian Relations, in: Holzer J., Mareš M. (eds.), Czech Security Dilemma. New Security Challenges, Palgrave Macmillan, Cham, Switzerland. https://doi.org/10.1007/978-3-030-20546-1_2

Mumford A. (2013) Proxy Warfare and the Future of Conflict, The RUSI Journal, No. 2, pp. 40–46, https://doi.org/10.1080/03071847.2013.787733

Potemkina O.Yu. (2020) Mnogourovnevoe upravlenie migracijey v Evropejskom soyuze. [Multilevel Governance of the EU Migration Policy], Sovremennaya Evropa, No 2(95), pp. 100–110, http://dx.doi.org/. (In Russian). https://doi.org/10.15211/soveurope22020100110

Seaman J. (2021) Towards a more China-centred global economy? Implications for Chinese power in the age of hybrid threats, Hybrid CoE Paper 9, The European Centre of Excellence for Countering Hybrid Threats, Helsinki, Finland.

Shishelina L.N. (2021) Tribom’e: postpandemicheskoe probuzhdenie. [The 3 Seas Initiative: Post-Pandemic Awakening], Nauchno-analiticheskij vestnik IE RAN, No 22(4), pp. 24–29, http://dx.doi.org/. (In Russian). https://doi.org/10.15211/vestnikian420212429

Simons G. (2021) Operational implications and effects of informational and political dimensions of western hybrid warfare, Bulletin of Moscow Region State University (e-journal), No. 3, URL: https://evestnik-mgu.ru/en/Articles/Doc/1078 (accessed: 30.11.2021)

Smirnov P.E. (2020) Evolyuciya politicheskih prioritetov SSHA v regione Baltijskogo morya vo vtorom desyatiletii XXI veka. [The evolution of US political priorities in the Baltic Sea region in the 2010s], Baltijskiy region, No 12(3), pp. 4–25, http://dx.doi.org/. (In Russian). https://doi.org/10.5922/2079-8555-2020-3-1

Svárovský M., Janda J., Víchová V., Gurney J. and Kröger M. (2020) Multilevel Governance of the US Migration Policy, https://doi.org/10.15211/vestnikian420212429

Translated by B. Alekseev