RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

EUROPEAN UNION FACING HYBRID THREATS

KAKHA GOGOLASHVILI

EXPERT OPINION 121

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

EXPERT OPINION

KAKHA GOGOLASHVILI

EUROPEAN UNION FACING HYBRID THREATS

121

2019

The publication is made possible with the support of the US Embassy in Georgia. The views expressed in the publication are the sole responsibility of the author and do not in any way represent the views of the Embassy.

Technical Editor: Artem Melik-Nubarov

ISSN 1512-4835
ISBN 978-9941-8-1205-7

Introduction

Hybrid warfare tactics are not new – their certain components have been used throughout history. Practically all types of actions that weaken opponents (or someone who is perceived to be an opponent) without using kinetic weapons, damage their unity, bring disorder to their structures and political processes, hinder the efficiency of their infrastructure, economic or institutional systems; sow panic and confusion or make it more difficult to govern society on certain territories – can be called hybrid warfare tactics. According to the classical (currently accepted) definition, hybrid warfare can be conducted both through conventional as well as non-conventional means (the terms "linear" and "non-linear" are also used in this regard); however, its ultimate goal is to occupy or seize territories.[1] Conventional tactics include the customary means of conducting warfare while hybrid tactics contain cyber and other non-traditional means of warfare. War situations in the 1990s in the Western Balkans and, especially Abkhazia and Transnistria, became polygons for formulating and testing hybrid warfare tactics. In these conflicts, the Russian security structures used various methods, be they presenting disguised troops as rebels, implementing their military plans by separatist forces in other countries, sowing panic by spreading rumors and disinformation or disseminating hate and alienation between artificially opposed camps.

All this "worked" quite efficiently; however, at today's stage, better and more efficient methods of dealing damage to the opponent have appeared and been established, including targeted cyber-attacks (both for gathering classified information as well as damaging critical infrastructure), the industry of spreading fake messages and disinformation in which (in Russia's case) scientific-research centers are also involved, planting influential agents in the political circles of opponents, the NGO sector and the media, and using economic and energy influence for political purposes and much more.

There is another important factor characteristic to hybrid tactics – the difficulty of their identification, especially when the result does not follow immediately. It is also complicated to precisely establish who conducted the attack and what specific purpose it served.

It is clear that at this stage only Russia uses the systemic approach to conducting hybrid warfare. It simultaneously brings together various tactical means and uses them in synergy for reaching a single (military) goal.

Neither the member states of the European Union nor its institutions realized the fact that Russia had been conducting hybrid warfare against

them for quite some time. This war was probably launched by Russia in 2011-2012;[2] however, the European Union did not openly recognize the threat coming from Russia until 2015 nor was it planning on taking any active measures to protect itself from this threat in a systemic manner.

Despite this, the EU policies that were focused on ensuring the Union's domestic security from the 1990s, also expanding to the issues of external security and defense from 2001, facilitated the preparation for these kinds of threats which are recognized as elements of hybrid threats today. However, the EU considered the source of such threats not to be Russia or any other state but rather terrorist or criminal groups and extremist organizations.

The Russian seizure of Ukrainian territories in 2014 by using hybrid tactics played the role of an important catalyst for the European Union to realize the real threats of hybrid warfare and develop defense systems against it.

Early EU Policies

Up until 2015, the EU's answer to hybrid threats was established neither in terms of definitions and their identification nor in terms of a unified policy instrument against it. However, the following can be considered to be steps in these directions:

- Recognizing the importance of new, non-military threats which first appeared in the 2003 EU Security Strategy.[3]
- The interconnectedness of external and domestic threats which was first recognized in the Political Guidelines adopted by Jean Claude Junker.[4]
- Uniting the efforts of member states for dealing with non-military threats and the necessity of coordination as discussed in the 2001 European Council Laeken Declaration. The declaration was adopted in response to the September 11, 2011 terrorist act in the United States.[5]
- Initiating cooperation in the fields of the judiciary, police, intelligence and sectorial structures.
- Steps taken after 2008 for protecting critical infrastructure.

At this stage, the policies were not yet being focused on hybrid threats specifically as there was no critical mass of actions that would cause qualitative changes in the attitudes of EU member states and institutions vis-à-vis their security.

Appearance of Hybrid Warfare in the EU Neighborhood

In 2014, Russia used hybrid warfare tactics for occupying and annexing Crimea – using propaganda, spreading lies, the active penetration by special forces, attacks on military objects using the civilian population, cyber-attacks on critical infrastructure, manipulation of criminal elements, actions of masked and disguised militarized elements and afterwards – direct military intervention.

Presumably at that time, the EU realized that its institutional system was not ready to eradicate such a complex threat if it were to apply to an EU member state; more specifically, if the following elements would be used:

Propaganda which was actively propagating the idea of the "Russian world" by TV and social media, discrediting the new Ukrainian government, convincing the Russian-speaking population of Crimea and other regions that terror would be used against them.

Activities of Special Forces. For years, the Russian intelligence had been planting secret agents of its influence in Ukraine, its institutions and military forces. During the annexation of Crimea, this brought results – numerous military and other officials as well as parts of the population openly supported the Russian aggression. Russian intelligence acquired information that made it practically impossible to defend military and civilian assets during the occupation.

Supporting pro-Russian oligarchs and subverting parties such as the Communist Party of Ukraine, Progressive Socialist Party of Ukraine and NGOs – Rodina (Russian blog), Rusich, Russkaya Obschina Krima, Ruski Mir and Oplot, and using them for specific purposes.[6]

Terrorist attack and crime. These methods were and are especially intensively used in Eastern Ukraine.

Cyber-attacks. According to the opinion of analysts, the "cyber capacities were minimally used for achieving kinetic results" in the war waged by Russia against Ukraine.[7] Despite this, means of cyber warfare were being used for obtaining classified information or damaging critical infrastructure.

Since 2011-2012 when Russia accused the United States of inspiring mass protest meetings in Moscow, the public (neither in Russia nor beyond its borders) did not believe the Kremlin's version after which a view was circulated within the Government of Russia that "in the 21st century, security policies are closely linked with dominating and manipulating information sources."[8] The strongest part of its information policy became spreading fake news. Certain aspects and principles of such types "of

undermining campaigns were being used back in the Cold War; however, their recognition (on the modern stage) and acknowledgement by Western publics and their governments was happening quite slowly."[9] Giles (Keir Giles, 2018) points out that Russia interferes in its neighborhood primarily through information and influence operations. For this, it uses its own third party media sources, cyber-hackers, business interests, NGOs, the Russian community and the funding of political parties, thereby undermining the process of the development of democracies and transparent decision-making in certain countries which are members of NATO and the EU.[10] The fact of the more frequent interference of Russian intelligence and security services with third countries is also indicated by another author, Ivo Juurvee (Juurvee, 2018), who says that the proof of this is the increasing discovery of Russian security agents working in third countries and qualifying their actions as "human intelligence" (HUMINT) while the usage of so-called "active measures" is also clear.[11]

Formulating Policies

The EU started actively talking about the necessity for dealing with hybrid threats in 2014-2025. A coherent vision for this first appeared in 2015 in the analytical document, entitled Countering Hybrid Threats,[12] formulated by the Office of the High Representative for Foreign Affairs and Security Policy. The document pointed out that the security environment of the EU changed significantly from 2014 for two reasons:

- In the East – Russian aggression in Ukraine which became a challenge to international order.
- In the South – ideological threats created by Daesh.

The document discussed at the PSC[13] made the concept of **hybrid war** clearer and characterized it as "overt or covert tactics managed through military or non-military means (intelligence/espionage, cyber operations, economic and so on) by which the attacker attempts to undermine the opponent. In order to achieve the goal, they use sabotage, damaging communications,[14] including energy and other systems, as well as supporting rebel and other groups, invading[15] other countries under the disguise of humanitarian intervention or holding a mass disinformation campaign against them as a result of which political influence or total control over the country is achieved."

A hybrid attack is usually aimed at the weaknesses of the country. In this context, the European Union External Action Service (EEAS) recommends member states to identify these kinds of weaknesses. One of the main weaknesses was assessed to be their economic and energy dependence

on external actors, the complete dependence of fields like finance, energy or transport on the proper functioning of critical infrastructure and its resilience. Cyber threat was important for whole EU due to its high level of internal cohesion. The less diversification of the energy sources of certain member states was also considered to be a problem.

Despite the fact that the process of revealing "weak points" towards hybrid threats was still a work in progress in the EU, they were already at the same time (2014-2015) trying to formulate responses to threats. In this context, four main issues were outlined:

a) **Being more informed**. Knowing more about one's own weak and vulnerable sides as well as that of others for which they had to create an internal "virtual space" to ensure early warning.

b) **Resilience.** The popular view among the EU institutions considers strengthening the resilience of member states for dealing with hybrid threats to be one of the primary means. In the case of an open aggression, member states were supposed to be able to use not only national instruments but also the support of those international organizations and military-defensive alliances of which they were a part.

c) **Containing aggression**. In order to make the motivation for the aggression of an opponent disappear, it is necessary to demonstrate that those who commit such acts will have to pay a high price – punishment or more for these wasted efforts.

d) **Answer to the attack.** During a hybrid threat it is difficult to draw a hard line between domestic and external security as well as civilian or military defense. Hence, it is also necessary to simplify the procedures of political decision-making at the EU level as well as having a powerful communication strategy.

On May 18, 2015, the Council of the European Union, meeting on the issues of defense and security, made important decisions.[16] The Council's Conclusions indicate that the links between external and internal security need to strengthened together with the synergy between defense and security services and structures in other fields of EU policy. The main threats are listed as: terrorism, organized crime, fighters who went abroad, contraband and human trafficking, chaotic migration, border control, energy and cyber security and so on. The Council requested the High Representative to prepare a joint framework action plan together with other EC services and the European Defense Agency (EDA)[17] by the end of 2015, helping the EU and its partners and neighbors in dealing with hybrid threats and boosting their resilience.

EU Action Plan in the Field of Hybrid Threats

From 2016, the formulation and realization of a clear, joint and integrated approach begins. In April, the External Affairs Council discussed and adopted the joint communication of the European Commission and EEAS (July)[18] which offered 22 specific actions to the EU and its member states for dealing with hybrid threats. The introduction of the document says that hybrid threats are the issue of defense and security and reacting to them is the sphere of the exclusive competence of EU member states; however, dealing with their entirety requires common EU efforts and the clauses of the Lisbon Treaty,[19] connected to the obligations of mutual defense and solidarity, are cited in this context. The document brings together all types of hybrid threats known at the time. Most of the activities are collective and require the coordinated actions of EU member states, institutions, organizations, agencies, projects and programs. The plan outlines goals such as: studying the nature of hybrid threats, organizing EU responses to challenges in terms of raising knowledge/perception and building resilience, crisis prevention, response and resolution, and developing cooperation with NATO. However, all of these goals are divided into tactical sub-goals (strategic communication) and the fields where appropriate action is required are underlined. The plan also clearly defines the places and responsibilities of the actors. The document also avoids duplication and hence it widely incorporates the activities ongoing in terms of other programs, plans and strategies, tailoring or adapting them for hybrid threats. Where necessary, the plan envisages the creation of new structures (such as the Hybrid Fusion Cell) or the strengthening of the already existing structures through new resources.

See the plan's structure presented in Annex 1. It must be pointed out that the European Council adopted the new EU security strategy (A Global Strategy for the European Union's Foreign and Security Policy) in November 2016. The Strategy, whose main line is societal resilience, also outlines the need for strengthening and further boosting the resilience of regional partners. The Strategy touches upon the issue of hybrid threats numerous times and considers dealing with them as important as developing other elements of the Union's defense.

Instruments for Managing the Fight against Hybrid Threats

Due to the EU Defense and Security Policy being the exclusive competence of the member states, the EU will not be able to completely centralize the fight against hybrid threats. Any activity performed within the EU in this regard requires the good will of the member states. However, on

the issues where consensus has already been reached and joint actions have been agreed on within the European Council or the Council of the European Union, EU institutions and services have the legitimate right to act in the name of all member states. Let us briefly discuss the instruments within and outside EU institutions which have been created for effectively countering hybrid threats:

EU East StratCom Task Force. Created on March 19-20, 2016. It aims to counter the Russian disinformation campaign. It acts in accordance with the 2015 EEAS Strategic Communication Action Plan. Its main tasks include:

- Efficient communication and introducing EU policies to the Eastern neighborhood.
- Improving the media environment in the Eastern neighborhood.
- Strengthening EU capacities in response to disinformation conducted by external actors.

The most disseminated product of this force is the weekly Disinformation Review[20] which analyzes the most recent messages from the Kremlin.

EU Hybrid Fusion Cell, which was created under the umbrella of the EEAS Intelligence and Situation Analysis Center (EU INTCEN),[21] is a part of the common EU plan for countering hybrid threats. Its goal is to analyze information about hybrid threats from open or closed sources.[22]

The Director of the EEAS INTCEN is the main person responsible for the activities of the Hybrid Fusion Cell. He is the main addressee of the reports and after a quick analysis and risk assessment (in terms of classified information) upon necessity, he supplies the received information to operative or decision-making services. He, as a rule, has constant connections to the so-called inter-service groups such as Countering Hybrid Threats (CHT) and the Community Capacity in Crisis Management (C3M). The member states also have their contact officer (with access to EU classified information) at the Council Secretariat who is being informed with regard to the established threat.

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).[23] The issue of the creation of the **Hybrid CoE** was also decided through the common plan for dealing with hybrid threats but is also in accordance with the joint EU-NATO Wales Declaration (2014). The Centre (situated in Helsinki, Finland) is not directly involved in avoiding actual threats or operative actions for avoiding them; however, it is heavily relied upon as an instrument which, through its research, will help the EU and NATO in understanding such threats, formulating responses to them,

educating the appropriate services in the EU, NATO and their member states in this regard and having close cooperation with expert circles and academia.

European Union Agency for Network and Information Security (ENISA). The ENISA is located in Greece in Athens and Heraklion. It was established in 2004 and actively facilitates the development of the network and information security in all of the EU. Its main task is to ensure the unhindered functioning of the EU single market which means close cooperation with the private sector for better protecting information networks. The Center also helps member states in formulating national cyber security strategies.

The 2016 joint staff working document, Operational Protocol for Countering Hybrid Threats,[24] also names other main instruments and structures participating in decision-making processes when it comes to hybrid threats. These include: ARGUS – EC rapid alert computer system (since 2005), CERT-EU – Computer Emergency Response Team, a part of the wider EU CSIRT7[25] network; ERCC – EC Emergency Response Coordination Centre, EU SITROOM – EU INTCEN Directorate, which has operative response capacities to crises; IPCR – the Integrated Political Crisis Response mechanism[26] and ISAA – Integrated Situational Awareness and Analysis.

The connection between these structures and mechanisms is well-reflected in the hybrid threat information exchange diagram presented in Annex 2.

Progress Achieved in Fighting Hybrid Threats

In this short period of time (2016-2018), the issue of chemical, biological, radiological and nuclear security (CBRN)[27] has become the most important in terms of the hybrid threats which were discussed in the 22-point plan (food safety, water and air pollution and healthcare context). The actualization of the issue was caused by the usage of a poisonous substance by Russian special forces in 2017 in Salisbury, UK. In 2017, the Council of the European Union adopted a separate action plan[28] which aims to increase EU resilience against chemical, biological, radiological and nuclear security risks. The issue of cyber security has become much more pronounced for the past two years. The 2017 joint EEAS and EC communication, entitled Building Strong Cyber Security for the EU, is a further testament to this.[29]

On June 13, 2018, the EC and EEAS prepared an annual report[30] on the implementation of the plan for countering hybrid threats, presenting it to the Council of the European Union and the European Parliament, which underlines progress in all priority areas such as: situation analysis and knowledge, creating resilience, EU and member state ability to rapidly

respond to crisis and counter it in coordination and strong cooperation with NATO. The document widely covers EU institutions and measures taken by the member states which are to ensure the better protection of critical infrastructure including nuclear and natural gas deposits, electrical grids and others. Both legislative as well as operative capacities for incident prevention on transport networks, naval or air transport have been strengthened and the newly established services for gathering and processing information have become more active, together with the security of cosmic observation. The coordination between civil security, healthcare and state security systems has been strengthened. Various measures have been taken for boosting cyber security including defense systems in state institutions. Plans for cooperating with the private sector have been developed. Measures for eradicating the funding for terrorism became more refined with the same being true for the resilience against hybrid threats against all important sectors. Special attention was paid to cooperation with third states; first of all, NATO partners and its neighborhood. EU services conducted many trainings and informational meetings in Eastern Partnership states. The instruments of EU decision-making have become more refined and moved to a regime of more coordination and rapid action. Close cooperation was established with NATO in terms of which a number of joint actions were conducted including joint exercises. In terms of **strategic communication**, progress is less notable; although East StratCom actively worked for neutralizing the threats. Further strengthening of cyber security has been presented as a task of the first order. Insufficient investment is considered to be a challenge for efficient cyber security. In 2018, the EC formulated recommendations which member states will use for coordinating response to large-scale cross-border cyber incidents and crises. Better sharing of intelligence information is also absolutely necessary. Insufficiently protected network connection between EU institutions and their representations abroad is recognized to be a weakness and is currently under intensive work. Resilience to hostile intelligence services is also being discussed as one of the increasingly important challenges. In this regard, strengthening security measures in EU institutions is considered to be a must. The employee accreditation system will become stricter and closer relations will be established between the appropriate services of member states.

General Conclusions

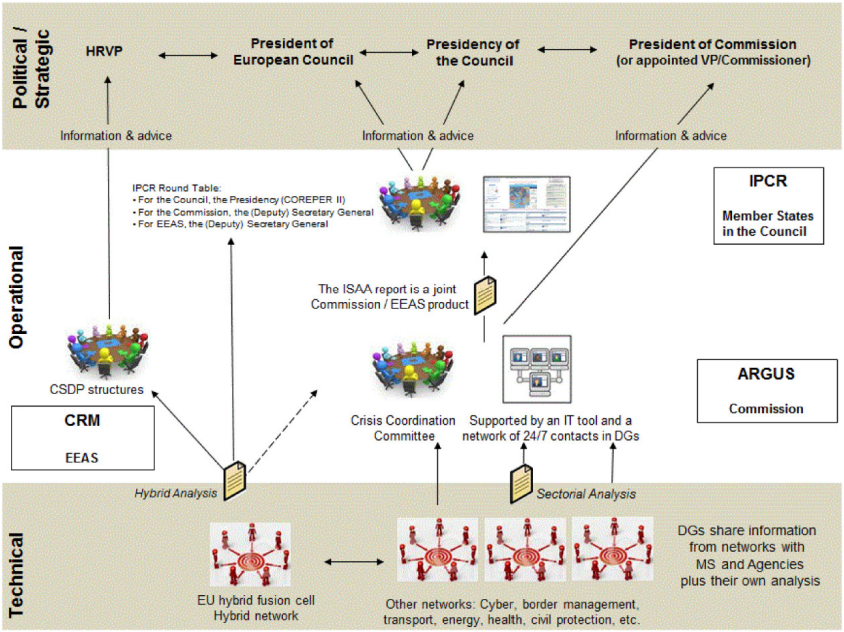
Hybrid warfare, waged by Russia against the European Union, is strategically still in favor of Russia despite the increasing EU response. There are several reasons for this:

- Russia is attacking and the EU is attempting to defend itself. It strengthens defense measures, creates more services, processes information, analyses the results and creates resilience. Yet, all of this is costing a lot while the attacks conducted by Russia are much cheaper.
- Defense in a situation when you do not know where the opponent will attack takes place only after discovering the harm. Despite the fact that the effect is determined relatively quickly, certain damage has already been done.
- Developing defense measures itself implies alternative expenditure which hinders the mobilization of resources in other areas as well as the overall development of the EU.
- EU response – institutional buildup and developments are practically open (except the information kept by specific structures). Hence, the opponent knows, simply through the assessment of EU institutions (it does not even need to spend resources on intelligence), where the weak points are and where the EU plans on doubling its efforts.
- At the same time, it is precisely this openness that creates EU moral strength. Yet such strength "works" only until the conflict enters the "phase of violent confrontation." If Russia manages to mobilize other large yet less democratic countries against the West, the opinion of the international community for it will be divided into "us" and "them" and then, only force and destructive capacities will decide everything. This second coalition will not find it necessary to heed any moral values, considering it as a mere weakness in the face of such confrontation.
- The EU must move to counter-attack tactics, yet it must not become like Russia for this which is harming its population and its institutions. This may also be the Russian state's goal – to turn the EU into such a destructive actor as itself. If in response the EU starts damaging Russia's critical infrastructure, threatening its population, spreading disinformation against Russia and its institutions and undermining their work through fake messages, then the opinion will emerge in the Russian public that "they were right" that EU is "an evil power."
- Involvement of the EU in this hybrid warfare, which is mainly defensive in nature, must signal more consolidation of this organization and more centralization and unification of its decision-making apparatus.
- This could become the reason for the full integration of the EU's defense and security.

Annex 1. Action Plan against Hybrid Threats

Strategic Goals	Tactical Goals	Target Fields
Studying the nature of hybrid threats (Act. 1)		
Organization of EU response: Boosting knowledge/understanding (Act. 2-4)	EU Hybrid Fusion Cell	
	Strategic Communication	
	European Centre of Excellence for Countering Hybrid Threats	
Organization of EU response: Building Resilience (Act. 5-18)	Protecting critical infrastructure	Energy networks
		Transport and supply network security
		Cosmos
	Defense capacities	
	Public health and food safety	
	Cyber security	Industry
		Energy
		Strong Financial System
		Transport
	Limiting hybrid threat funding	
	Resilience to radicalization and violent extremism	
	Cooperation with third countries	
Crisis prevention, response and resolution (Act. 19,20,21)		
Developing cooperation with NATO (Act. 22)		

Annex 2. Information Exchange about Hybrid Threats



Source: European Union External Action Service

References

1. "Nonlinear Warfare," 2019, *Global Security Review*, www.globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/
2. Stefan Meister (DGAP, Berlin), "Disinformation as Part of Russia's Security Strategy," *Hybrid Conflict: The Roles of Russia, North Korea and China*, Edited by: Frans-Paul van der Putten, Minke Meijnders, Sico van der Meer and Tony van der Togt, p. 8.
3. "A SECURE EUROPE IN A BETTER WORLD," *EUROPEAN SECURITY STRATEGY,* Brussels, 2003. www.internationaldemocracywatch.org/attachments/307_European%20Security%20Strategy.pdf
4. www.ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech_en.pdf
5. Conclusions and Plan of Action of the Extraordinary European Council Meeting (21 September 2001). www.cvce.eu/en/obj/conclusions_and_plan_of_action_of_the_extraordinary_european_council_meeting_21_september_2001-en-a012ede7-96d9-4c37-a7ce-cae949ddf401.html
6. Jurij Hajduk and Tomasz Stępniewski, 2016, "Russia's Hybrid War with Ukraine: Determinants, Instruments, Accomplishments and Challenges," *Studia Europejskie*, 2/2016. p. 7. www.ce.uw.edu.pl/pliki/pw/2-2016_hajduk.pdf
7. J. A. Lewis, 2015, *Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine*, Centre for Strategic and International Studies (CSIS). p. 41.
8. Stefan Meister (DGAP, Berlin), "Disinformation as Part of Russia's Security Strategy," *Hybrid Conflict: The Roles of Russia, North Korea and China,* Edited by: Frans-Paul van der Putten, Minke Meijnders, Sico van der Meer and Tony van der Togt.
9. Keir Giles, 2015, *Russia's Hybrid Warfare: A Success in Propaganda*, Arbeitspapier Sicherheitspolitik, Nr. 1. p. 1. www.researchgate.net/publication/280922184_Russia's_Hybrid_Warfare_A_Success_in_Propaganda
10. Keir Giles, 2018, "Russia, Influence and 'Hybrid,' *Hybrid Conflict: The Roles of Russia, North Korea and China.* Edited by: Frans-Paul van der Putten, Minke Meijnders, Sico van der Meer and Tony van der Togt, p. 5.
11. Ivo Juurvee, 2018, *The Resurrection of 'Active Measures:' Intelligence Services as a Part of Russia's Influencing Toolbox*. Hybrid CoE. Analysis April 2018, p. 4. www.hybridcoe.fi/wp-content/uploads/2018/05/Strategic-Analysis-2018-4-Juurvee.pdf
12. Food-for-thought paper, «Countering Hybrid Threats,» European External Action Service (EEAS) To: Political and Security Committee (PSC), Brussels, 13 May 2015.
13. EU Political and Security Committee (at the Council of the European Union).
14. Such an attack took place against Georgia in 2006 when Russian special forces blew up the Georgia-Russia gas pipeline.

15. Such a tactic was used by Russia against Georgia in 2008; however, it was not assessed as hybrid warfare by anyone at the time. Later, the same tactics were used in Ukraine (author's remark).

16. COUNCIL CONCLUSIONS ON CSDP, Foreign Affairs Affairs Council, 18 May 2015, Brussels, 18 May 2015 (OR. en) 8971/15.

17. European Defence Agency, www.eda.europa.eu/

18. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response, Brussels, 6.4.2016 JOIN(2016) 18 final.

19. The last founding EU treaty signed in 2009. Technically two treaties: Treaty on the European Union (TEU) and Treaty on the Functitoning of the European Union (TFEU) that regulate the division of competencies between EU institutions and member states, representing the source of EU laws.

20. *Disinformation Review.* www.euvsdisinfo.eu/disinfo-review/

21. EU INTCEN is one of the EEAS Directorates which is subject to the Deputy Secretary General for Crisis Management and CSDP. Its tasks include: analyzing the information supplied by the security and intelligence services of member states, research/analysis of open sources, analyzing information in all sorts of crises and connections with decision-makers and consular crisis management (issues of protecting EU citizens in case of crisis). See: www.statewatch.org/news/2016/may/eu-intcen-factsheet.pdf and also www.cdn4-eeas.fpfis.tech.ec.europa.eu/cdn/farfuture/nrjtrUn55rD6QWxYjQJmMHjABORlWfbWKXuNpTdz3Yo/mtime:1549012543/sites/eeas/files/2019-01-02_-_eeas_2.0_orgchart.pdf

22. Parliamentary questions, 12 January 2018, answer given by Ms. Bieńkowska on behalf of the Commission. www.europarl.europa.eu/doceo/document//E-8-2017-005865-ASW_EN.html

23. www.hybridcoe.fi/what-is-hybridcoe/

24. JOINT STAFF WORKING DOCUMENT EU operational protocol for countering hybrid threats 'EU Playbook,' Brussels, 5.7.2016 SWD(2016) 227 final. www.statewatch.org/news/2016/jul/eu-com-countering-hybrid-threats-playbook-swd-227-16.pdf

25. Computer Security Incident Response Team.

26. Integrated Political Crisis Response.

27. Chemical, biological, radiological and nuclear related threats.

28. Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, Brussels, 18.10.2017 COM(2017) 610 final.

29. Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU. Brussels, 13.9.2017 JOIN(2017) 450 final.

30. On the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018. Brussels, 13.6.2018 JOIN(2018) 14 final.