# Policy Integration Across Multiple Dimensions: the European Response to Hybrid Warfare

Stoian, Valentin

# Policy Integration Across Multiple Dimensions: the European Response to Hybrid Warfare

**VALENTIN STOIAN**[*]
("Mihai Viteazul" National Intelligence Academy)

**Abstract**

The article analyzes the European Union's response to hybrid warfare and argues that a proper interpretation of the policies adopted offers cautious support for a rational choice intuitionalist approach. It begins with the presentation of the main theories of European decision-making, among which rational choice and constructivist institutionalism and it derives a hypothesis which it tests in the third part of the article. Several policy documents are analyzed in order to provide the empirical material for the analysis. The article concludes that EU institutions prefer to undertake supra-national action in technical fields which are less politically controversial and where supra-nationalization is more easily accepted.

**Keywords:** hybrid warfare, constructivism, institutionalism, spill-over.

## Introduction

The 2014 annexation of Crimea by the Russian Federation, as well as the beginning of the Donbas conflict represented a relevant turning point in EU policy making. These challenges required a response from the institutions of the Union, given that two member states, Latvia and Estonia share a direct border with the Russian Federation, while others, such as Romania and Bulgaria have a coastline on the Black Sea. In 2016, the European Commission and the High Representative presented to the European Parliament a policy document entitled the *Joint Framework on countering hybrid threats*,[1] which included a varied set of replies to the evolving challenge.

[*] Valentin Stoian is a researcher in Political Theory with the "Mihai Viteazul" National Intelligence Academy (valentin.stoian@animv.ro, stoian.valentin@animv.eu).

[1] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint communication to the European Parliament and the Council: 'Joint Framework on countering hybrid threats - a European Union response'," JOIN(2016) 18

The concept of “hybrid warfare” was coined to describe the tactics that Russian Federation employed against NATO and the EU states.[2] While it has been heavily criticized in the literature,[3] “hybrid warfare” captures, to some extent, the diversity of means that the Russian Federation has employed. The Russian strategy in Crimea used a combined set of military, economic and information warfare,[4] which helped the Russian Federation obtain a quick victory. Furthermore, the use of information warfare was documented in the 2016 US elections,[5] as well as in the Brexit referendum that took place the same year. Other, less intrusive attempts at interference occurred in the case of the 2017 Italian elections,[6] as well as in the 2018 Hungarian ones.[7] The most recent incident was the attempted assassination of the ex-GRU colonel, Serghei Skripal and of his daughter Yuliya, that took place in Salisbury, UK as well as the attempted sabotage of the investigation into the incident by the Russian GRU.[8]

The article will analyze the European Union’s policies for combating hybrid warfare through the lenses of contemporary European decision-making theories and will argue that the re-emergence of the Russian threat has provided the supra-national institutions of the Union with an opportunity to assert and even extend their power. The article will argue that policies adopted to combat Russia’s hybrid warfare offer support for a rational-choice institutionalist perspective of interpretation of European decision-making. The analysis will

final, 2016, accessed July 14, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

[2] Alexander Lanoszka, “Russian hybrid warfare and extended deterrence in eastern Europe,” *International Affairs* 92, no 1 (2016): 175-195, Martin Kragh and Sebastian Åsberg, “Russia’s strategy for influence through public diplomacy and active measures: the Swedish case,” *Journal of Strategic Studies* 40, no 6 (2017): 773-816.

[3] Bettina Renz, “Russia and ‘hybrid warfare’,” *Contemporary Politics* 22, no 3 (2016): 283-300.

[4] Tony Balasevicius, “Looking for Little Green Men: Understanding Russia´s Employment of Hybrid Warfare”, accessed June 13, 2018, http://www.css.ethz.ch/en/services/digital-library/articles/article.html/1227f31f-370a-4051-83ca-3a04f97932be/pdf.

[5] House Permanent Select Committee on Intelligence, “Report on RuSsian Active Measures,” March 22, 2018, accessed June 10, 2019, https://docs.house.gov/mwg-internal/de5fs23hu73ds/progress?id=n65m50GVLvqRylNukkZqFsYqIKLxv9JJI5J4RbV772k.

[6] David Alandete and Daniel Verdú, “How Russian networks worked to boost the far right in Italy,” March 1, 2018, accessed June 13, 2018, https://elpais.com/elpais/2018/03/01/inenglish/1519922107_909331.html.

[7] Katalin Andor et al., “The impact of Russia’s state - run propaganda apparatus on online media in Hungary - 2010–2017,” March 2018, accessed June 13, 2019, http://www.crcb.eu/wp-content/uploads/2018/05/crcb_2017_mrsrpphnm_English_180319_.pdf.

[8] Government.nl, 2018, “Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW,” accessed July 20, 2019, https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw.

rely on a set of policy documents issued by the European Commission and will employ process-tracing in order to describe the development and trace the evolution of the European Union's policies for combating hybrid warfare.

The first part of the article will describe the theoretical framework which the article will employ. It will describe the main tenets of Ernst Haas' neofunctionalism and the concept of spill-over, rational choice and constructivist institutionalism and will derive the hypothesis that will be tested in the empirical part of the article. Further, a short presentation of the decision-making mechanisms under co-decision and the Common Foreign and Security Policy will be outlined. The theories presented will be compared on the basis of their conceptualization of the actors and of the way they predict actor behavior in the face of a policy challenge.

The second part of the article discusses theories of European decision making, while the third presents process tracing and shows how the article employs this methodology in order analyze the European Union's policies for countering hybrid threats. The fourth section will present the state of the EU's policies as they have developed since the 2016 adoption of the *Joint Framework on countering hybrid threats*.[9] The last section of the article will assess whether the hypothesis tested has been confirmed or rebutted by the empirical material. Furthermore, it will argue that the empirical material presented lends evidence to support a rational choice-institutionalist interpretation. The article's main finding is that both rational choice and constructivist institutionalism would predict an expansion of the power of supra-national institutions, but the former can better explain why supra-national integration is primordially achieved in technical and scientific policy areas.

## Theories of European Decision-Making

The following section will present an overview of three theories of European decision-making. It will discuss both their ontological fundamentals and their conceptualization the policy adoption process. Then, the architecture of European decision-making will be briefly presented, in order to understand the institutional positions of actors involved in combating hybrid threats and the incentives and identities that these operate under.

The main argument of the classical theory of neo-functionalism is that trans-national cooperation in a particular field leads to increased cooperation in

[9] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint communication to the European Parliament and the Council: 'Joint Framework on countering hybrid threats - a European Union response'," JOIN(2016) 18 final, 2016, accessed July 14, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

other policy fields, in a process called spill-over. According to this view, once cooperation between actors begins, it leads to an increased demand for regulation, which also supports cooperation in other fields and, which, in turn leads to more demand for regulation. According to Sandholtz and Sweet,[10] the process of integration takes place through "spillover" effects from one policy area to another.

The authors define the idea of "spillover" as "spillover occurs when actors realize that the objectives of initial supranational policies cannot be achieved without extending supranational policy-making to additional, functionally related domains."[11] This is similar to the definition offered by Philippe Schmitter in 1969, who argued that spillover is "the process whereby members of an integration scheme - agreed on some collective goals for a variety of motives but unequally satisfied with their attainment of these goals - attempt to resolve their dissatisfaction by resorting to collaboration in another, related sector (expanding the scope of mutual commitment) or by intensifying their commitments to the original sector (increasing the level of mutual commitment), or both."[12]

Another fundamental concept in the neo-functionalist theory is the idea of "stickiness." This means that rules, once enacted, create a series of actors interested in their maintenance. Thus, once a set of interests has been institutionalized, it becomes very difficult to roll them back given that actors have vested interests in defending them.[13]

Yet another result of integration is, in the view of neo-functionalist analysts, the emergence of supra-national interests. Not only do actors such as Member States or interest groups at the sub-national level (commercial interests, trade unions, political parties) cooperate at an accelerated rhythm, but the creation of supra-national institutions generates an interest that these have to perpetuate and increase their own power. Supra-national institutions generate positions, are served by a well-paid bureaucracy and act as places of elite socialization, where previously nationally-minded elites need to adopt a "European" identity. These institutions themselves then drive the integration process, aiming to extend their competences, both at the expense of Member States and at the expense of each other.[14] One example quoted in the literature is the pan-European networks of interests that the European Commission

[10] Wayne Sandholtz and Alec Stone Sweet, "Neo-functionalism and supranational governance," in Erik Jones, Anand Menon and Stephen Weatherill (eds.), *The Oxford Handbook of the European Union* (Oxford: Oxford University Press, 2012): 1-19.

[11] Sandholtz and Sweet, "Neo-functionalism and supranational governance," 15.

[12] Carsten Stroby Jensen, "Neo-functionalism" in Michelle Cini, Nieves Pérez-Solórzano Borragán (eds.), *European union politics* (Oxford: Oxford University Press, 2010): 71-86.

[13] Sandholtz and Sweet, "Neo-functionalism and supranational governance," 16.

[14] Jensen, "Neo-functionalism," 92.

assembles regularly, with the aim of proposing "European" solutions to problems and thus increasing the power of the Commission to the detriment of that of national governments.[15] A further example could be observed in the 2018 State of the European Union address by Commission president Jean Claude Juncker who argued for the increase use of Qualified Majority Voting in European Security Policy.[16] This would severely restrict the power of the Council of the European Union and of Member States that are represented in it, as foreign security policy represents the last policy field where a unanimity is needed to adopt decisions.

Classical neo-functionalism does not take any stand on ontological debates. Spill-over effects can be generated either by a set of rational actors taking advantage of the economies of scale generated by a wider market or by a process of common identity formation through socialization in supra-national institutions. Given its ontological silence, neofunctionalism can be adapted by both rationalist and constructivist inspired conceptions.

The second theory of decision-making that the article employs to understand the development of EU policies aimed to combat hybrid warfare is rational-choice institutionalism. Developed by Jon Elster, Douglas North and Ronald Coase, rational choice institutionalism argues that actors are, at least instrumentally, rational. This means that they are able to identify a certain goal (at the most basic level, the theory assumes that actor goals are relatively invariant and they can be subsumed under the idea of power maintenance and maximization) and optimize the means in order to achieve it. Furthermore, actors' rationality is bounded, in the sense that they employ the minimum required effort to acquire the information necessary for a decision and employ heuristic devices such as "rules of thumb, standing decisions, stopping rules, and satisficing."[17]

Rational-choice institutionalism embraces a positivist epistemology. Under its assumptions, the world is "composed of discrete objects that are independent from the observer"[18] and objective trends and phenomena exist and are identifiable by the respective observer. Thus, actors and their strategy are easily identifiable by the researcher and the result of their bargaining can be analyzed after a judicious coding of their initial preferences and the policy outcomes.

[15] Jensen, "Neo-functionalism," 92, Sandholtz and Sweet, "Neo-functionalism and supranational governance," 17.

[16] Jean-Claude Juncker, "State of the European Union 2018," September 2018, accessed July 20, 2019, https://ec.europa.eu/commission/priorities/state-union-speeches/state-union-2018_en.

[17] Kenneth A. Shepsle, "Rational choice institutionalism" in R. A. W. Rhodes, Sarah A. Binder, and Bert A. Rockman (eds.), *The Oxford handbook of political institutions* (Oxford: Oxford University Press, 2008): 24-26.

[18] Ariadna Ripoll-Servent, *Institutional and policy change in the European Parliament: Deciding on freedom, security and justice* (New York: Palgrave Macmillan 2015), 7.

Within this context, institutions (understood as sets of rules) represent either constraints on actor behavior or equilibrium results when a phase of institutional change occurs. They represent constraints in the sense that they determine the “rules of the game”, under which the actors pursue their rational goals. Therefore, according to this interpretation of rational-choice institutionalism, institutions limit or aid what an actor can do when attempting to achieve his goals (increase or decrease transaction costs, determine that an actor must include the interest of another in his decision-making, simplify information flows).[19] The simplest understanding of rational choice institutionalism has been presented as: “goal-oriented actors operat[e] within institutional constraints”,[20] where actors form their preferences exogenously.

According to rational choice institutionalism institutions can also represent equilibrium results. On this view institutions are not exogenous constraints, but the results of interaction between rational, power-maximizing actors. Thus, they reflect the power balance between particular actors at a particular time. Thus, when a new rule is made, actors’ bargain and the preferences of the stronger actor prevail and are institutionalized.[21]

Conversely, constructivist institutionalism employs a post-positivist epistemology and an interpretive methodology. According to this view, social entities “do not exist as an external unit but are socially constructed through perceptions, norms and discourses of social actors.” Thus, according to the proponents of constructivist institutionalism “social entities and actors are ‘mutually constituted’: structures, such as ideas and norms, constitute actors and their interests, but actors can also change and reformulate structures.”[22]

According to constructivist institutionalism, there is a much closer relationship between actors and structures, who are not necessarily separated. If, in the case of rational choice institutionalism, actors adapt their strategies to existing institutions, when constructivist frames are applied, the relationship thins. On the one hand, actors are defined by values and narratives, while, on the other, institutions are built to embody particular views of the world. Actors, according to this view, are defined by interests which are “social constructions that cannot serve as proxies for material factors.”[23] Thus, actors do not have exogenous preferences, they form preferences in relationship with the institution they operate under, by partially adopting the narrative of the institution. Alternatively, institutional change occurs when particular actors

[19] Shepsle, “Rational choice institutionalism,” 25.

[20] Ripoll-Servent, *Institutional and policy change*, 44.

[21] Shepsle, “Rational choice institutionalism,” 27.

[22] Ripoll-Servent, *Institutional and policy change*, 7.

[23] Colin Hay, “Constructivist Institutionalism”, in Rhodes, Binder and Rockman (eds.), *The Oxford handbook*: 56-74.

manage to frame a particular issue in such a way in which it is accepted by enough other actors to institutionalize it.

According to Ripoll Servent,[24] under constructivist institutionalism "the translation from policy preferences into policy outputs is done using framing as a mechanism for change." Thus, actors jockey to provide the most acceptable understanding of events through framing, which is understood as the process during which "definitions of a situation are built up in accordance with principles of organization which govern events (...) and our subjective involvement in them."[25] Frames compete among each other and are carried through by frame entrepreneurs, who push their own frame and attempt to modify the competing frames in order to achieve consensus on a particular issue. The position of the frame-entrepreneur within the system of symbolic power is crucial: a previously held position of power and the ability to show knowledge of a particular issue allows a frame entrepreneur to better adjust the framing of an issue to his or her preferred position.[26]

To summarize, the goal of constructivist institutionalism is to identify how, in the competition of ideas, some get institutionalized, while others get eliminated. According to Colin Hay "constructivist institutionalism thus seeks to identify, detail, and interrogate the extent to which—through processes of normalization and institutional embedding—established ideas become codified, serving as cognitive filters through which actors come to interpret environmental signals."[27]

Combating hybrid warfare takes place across several policy fields, each falling under a different decision mechanism. This makes the analysis of the comprehensive policy package extremely difficult, since each policy generates a different requirement for inter-actor agreement and a different "game" to be played between different actors. Within this policy package, several decisions involve the adoption or better implementation of EU-wide legislation (directives or regulations), others imply actions coordinated by the Commission but implemented by Member States, some are applied by the Commission's own agencies and subordinated institutions, while yet others, come under the Common Foreign and Security Policy, which is adopted unanimously by the Council of the European Union, based on a proposal from the High Representative.

Based on this short presentation of the EU's policy areas, one can define four ways in which EU institutions can act. These will be used in the analysis of the actual policies adopted by EU institutions. The first and most clear type of action EU institutions can take is the adoption of supra-national legislation through the ordinary legislative procedure or other similar procedures. The

[24] Ripoll-Servent, *Institutional and policy change*, 49.
[25] Ibid.
[26] Ibid, 50.
[27] Hay, "Constructivist Institutionalism," 65.

second option is the inter-governmental adoption of policies, which is a requirement in foreign and security policy. The third is supra-national action at below the legislative level through, for example, the use of one of the Commission's agencies or services to elaborate guidelines or to implement changes to its own mode of operation. Finally, the fourth and the least "supra-national" of them is the coordination of national policies whereby the Commission only adopts the role of a mediator and coordinator between the national governments.

The main aim of the article is to investigate whether rational-choice or constructivist institutionalism better explain the EU institutions' actions in combating hybrid warfare. In order to do this, it formulates a hypothesis based on the two theories.

Rational choice institutionalism claims that actors seek to maximize power but that they will take the minimum required risks. Thus, supra-national actors such as the Commission or the High Representatives will undertake policy initiatives in "technical" fields, which are governed by specialized personnel and where member states benefit considerably from increased cooperation. Thus, supra-national institutions will seek to present "unity" in front of an external threat but aim to supra-nationalize power in policy fields where less controversy is to be expected.

Alternatively, constructivist institutionalism sees actors as defined by their identity. In this case, where the Russian Federation is primordially defined as a "non-democratic" threat which is opposed to the "civilized West",[28] supra-national actors will make a "stand" in crucial foreign and domestic policy initiatives, which aim to reinforce the "democratic values" narratives held by European institutions. The existence of an "external threat" will allow the Commission or the High Representative to centralize power to the detriment of Member States in domains previously reserved to national prerogative such as foreign policy.

The article aims to test the following hypothesis, whose confirmation would lend support to rational choice institutionalism. Alternatively, evidence against the hypothesis would lend credence for constructivist institutionalism

In the context of hybrid warfare, the EU's supra-national institutions initiate policies in more "technical" and less "political" fields of policy-making.

## Methodology

Process - tracing aims to explain a certain policy result by determining and thoroughly investigating the relevant moments which brought it about and through the evaluation of potential explanations for that outcome. According to

[28] Glen Diesen, *EU and NATO Relations with Russia: After the Collapse of the Soviet Union,* (London: Routledge, 2015).

Bennett and Checkel, process-tracing relies on the "examination of intermediary steps in a process, in order to examine how that process took place and if that process led to a relevant result."[29] Similarly, according to Collier, process-tracing is similar to historical investigation, in the sense that relevant episodes are arranged in a temporal sequence.

Process-tracing can be used either to explain pre-existent theories or, in the absence of a theory to generate relevant hypotheses, to analyze crucial moments which led to the relevant result. If a higher-level theory is not used as an explanatory framework, an alternative is presenting competing hypotheses which explain the final result and testing them on relevant moments. From the point of view of data collection, process - tracing employs: 1. Document analysis 2. Interviews with political decision-makers 3. The analysis of relevant statements by political decision-makers, especially those made before relevant decision-making moments (which will be compared to the results of those decision-making processes- for example, negotiations that lead to the adoption of a particular treaty). According to Robinson the aim of process-tracing in the case of specific episodes is to investigate the way in which "particular configurations of idealized factors were combined in order to generate specific results."[30]

Bennett[31] describes process-tracing as "retroactive scenario analysis" and identifies a number of similarities between the two. Both are interested in small-scale decision-making, aiming to investigate what were or what will be the choices made by high-level officials, especially under the influence of external stimuli. However, the main difference between the two lies in their time-orientation: scenario analysis looks to identify potential future developments, while process-tracing looks towards the past in order to evaluate the relative importance of the determinants of a particular event. According to Punton and Welle,[32] process-tracing requires five stages:

> 1. Elaborating a hypothesis on the causal mechanism which achieved a particular result. This can involve the use of higher-level theories which allow for the generation of hypotheses or simply the enumeration of the potentially relevant determinants.

[29] Andrew Bennett and Jeffrey Checkel, *Process Tracing: From Metaphor to Analytic tool*, (Cambridge: Cambridge University Press, 2015), 20.

[30] Corey Robinson, "Tracing and explaining securitization: Social mechanisms, process tracing and the securitization of irregular migration," *Security Dialogue* 48, nr. 6 (2016): 505–523.

[31] Andrew Bennett, "Using Process-Tracing to improve Policy Making: the (negative) case for the 2003 Intervention in Iraq," *Security Studies* 24, nr 2 (2015): 228-238.

[32] Melanie Punton and Katharina Welle, "Applying Process Tracing in Five Steps," 2015, accessed October 3, 2019, https://opendocs.ids.ac.uk/opendocs/bitstream/handle/123456789/5997/CDIPracticePaper_10_Annex.pdf;jsessionid=8AAF83A109DB2372F412BC6CA0B67656?sequence=2.

2. The operationalization of the causal mechanism involves identifying the observable manifestations of a mechanism and of the empirical evidence which would allow us to state that the particular chain of events that the causal mechanism predicts actually took place.
3. The collection of empirical data through interviews or document analyses.
4. The evaluation of the explanatory power of each piece of evidence and the identification of their relevance (does it support, confirm, weaken or invalidate the theory).
5. The elaboration of conclusions on whether the hypothesized mechanism produced the particular result.

The article uses process - tracing based on document analysis. Thirteen relevant EU policy documents have been identified, which outline the plans and the progress of the European Union in combating hybrid threats. A wide approach was used, and the documents included did not refer only to hybrid threats *per se*, but also to specific areas of hybrid warfare such as disinformation and to specific measures adopted, such as creating resilience. The wide approach led to the inclusion of other policy documents such as the code of conduct for online platforms.

A system of analysis was elaborated which included the actors relevant for a particular action, as well as its nature (either a form of coordination of inter-governmental cooperation, inter-governmental policy making or the use of supra-national legislation) and a coding of the policy field in which the action is undertaken. Policy fields were coded as either “technical” or “political”, depending on whether they are more or less contested by relevant actors. The goal of this analysis is to identify whether supra-national action is carried out in more “technical” or more “political” fields of policy-making when combating hybrid threats. Finally, policy implementation steps were arranged in a chronological order, with the aim of identifying relevant junctures in policy roll-out and to form an overall picture on the evolution of the combating of hybrid warfare. Table 1 presents, the analysis of the policy documents which the European Union has issues on the topic of hybrid warfare.

## EU Policies - Combating Hybrid Warfare

The annexation of Crimea by the Russian Federation and the ignition of the Donbas war were first reflected in EU documents in a food-for-thought paper initiated by the External Action Service in May 2015 in preparation for the Foreign Affairs Council that month.[33] This document[34] suggested that the

[33] Council of the European Union, “European Council meeting (19 and 20 March 2015) – Conclusions,” accessed July 13, 2019, http://www.consilium.europa.eu/en/press/press-releases/2015/03/20/conclusions-european-council/, 2015.

Russian Federation's rapid victory over Ukraine was caused by the latter state's extensive vulnerabilities. According to the document, Russia's hybrid warfare (defined as the centralized use of both covert and overt tactics) exploited Ukraine's vulnerabilities such as:

> (i) weak governance and national institutions, wide-spread corruption;
> (ii) lack of trust and support for security and defense structures;
> (iii) the presence of a large Russian speaking population that perceived itself marginalized; and
> (iv) critical dependency on Russia for imports and energy supply."[35]

The food-for-though paper sees two steps in answering this challenge - the improvement of awareness capabilities (of both hybrid actions as well as one's own vulnerabilities), followed by the increase of resilience (diminishing one's vulnerabilities in order to better withstand stress and catastrophe). In order to achieve these goals, the document foresees a form of self-evaluation of vulnerabilities from the part of Member States, EU support through CSDP missions in neighboring states in order to increase resilience as well as cooperation with NATO (considering that the EU does not have mechanisms to respond to a conventional military attack).

Further, the paper foresees the creation of a EU fusion cell, with the aim of improving the secure exchange of information on hybrid attacks and on the vulnerabilities of member states, to improve the cooperation with NATO and to increase the strategic communication efforts that seek to combat the information component of hybrid warfare.[36]

The institutionalization of these efforts came through the Foreign Affairs Council Conclusions of June 2015, which addressed the topic of security and defense with the NATO Secretary General.[37] This represented the preliminary for the April 2016 Communication by the European Commission and the High Representative for Foreign Affairs and Security Policy, entitled *Joint Framework on countering hybrid threats: a European Union response.*[38] It constitutes the roadmap for the EU's policies against hybrid threats and is divided in five chapters and 22 actions. Three implementation reports have been

[34] Council of the European Union, "Food-for-thought paper 'Countering Hybrid Threats'," 2015, accessed July 6, 2019, http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf.

[35] Council of the European Union, "Food-for-thought paper."

[36] Ibid.

[37] Council of the European Union, "Outcome of the Council Meeting. 3389th Council meeting. Foreign Affairs - 18 May 2015," 2015, accessed July 13, 2018, https://www.consilium.europa.eu/media/23345/st08966en15.pdf.

[38] JOIN(2016).

issued in July 2017, July 2018 and May 2019, which show the progress of the Communication's actions and the areas where improvement is required.[39]

The Communication begins with an argument where the concept of hybrid threats is defined as the "mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes."[40] Further, the Communication argues that, while national security remains a responsibility of the nation-states, many of the threats that these face are common and require a coordinated response, thus paving the way for supra-nationalization of policies. The Communication also references other EU sectoral strategies such as "the European Agenda on Security, the upcoming European Union Global Strategy for Foreign and Security Policy and European Defence Action Plan, the EU Cybersecurity Strategy, the Energy Security Strategy and the European Union Maritime Security Strategy",[41] arguing that it represents merely a continuation and deepening of these efforts.

As can be seen in Table 1, the European Commission adopted a number of 22 policy directions and has, over the past three years, worked to implement them. They are divided into four main areas entitled: "Recognizing the Hybrid Nature of a Threat", "Organizing the EU response: improving awareness", "Organizing the EU response: building resilience".[42] "Preventing, responding to

[39] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats - a European Union response," 2017, accessed July 14, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0030&from=GA; European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint Report on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018," 2018, accessed July 14, 2019, https://eeas.europa.eu/sites/eeas/files/joint_report_on_the_implementation_of_the_joint_framework_on_countering_hybrid_threats_from_july_2017_to_june_2018.pdf; European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 2019 "Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats," 2019, accessed July 14, 2019, https://eeas.europa.eu/sites/eeas/files/report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilien.pdf/

[40] EC/EEAS, "Joint Framework on countering hybrid threats."

[41] Ibid.

[42] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint communication to the European Parliament and the Council: 'Joint Framework on countering hybrid threats - a European Union response'," JOIN(2016) 18

crisis and recovering". The first dimension involves only one policy dimension and asks member states to determine their own vulnerabilities through a questionnaire addressed to all governments. The second dimension looks to improve the awareness of both institutions and the population regarding disinformation campaigns and dangerous propaganda, through measures such as the establishments of a Hybrid Fusion Cell, improved strategic communication, and the analysis provided by the Helsinki Center for combating hybrid threats. Building resilience comes next and it involves, according to the European Commission, a wide approach to the concept, which includes the resilience of institutions, people and critical infrastructures. Finally, on the recovery side, the action plan involves establishing operational protocols for crisis management and testing them through common exercises with NATO, as well as investigating the EU's military capabilities.

The differential roll-ut of the policies is presented in Table 1. While some began quickly after the adoption of the Communication, others required more time for consultation and debate before they could be formalized in official legislative acts. For example, the creation of the EastStratcom cell within the EEAS was implemented rather quickly, while the creation of a set of indicators which detail the vulnerability of critical infrastructures or the creation of guidelines for screening foreign investments and the adoption of a regulation on it took until 2019. EU-NATO cooperation was strongly increased due to the fact that both institutions placed the resurgence of the Russian Federation high on the scale of potential threats.

Furthermore, the European Commission took separate actions against online disinformation. The first step undertaken by the Commission was the formation of a High Level Expert Group on fake news. This group aimed to analyze the way fake news spread, the roles and the responsibilities of relevant actors and to formulate recommendations of how this phenomenon can be fought.[43]

The report of the High Level working group was issued in March 2018 and includes a set of analyses and policy recommendations. The report defines misinformation and disinformation differently and argues that the first is truly dangerous because it constitutes an intentional and clear action with the aim of causing a damage or to obtain a profit. The report argues that civil society should act as a "watchdog" of democracy (supervising the actions of state and private actors) and that, a part of information that is spread is relayed further by citizens, especially given the emergence of electronic mass-media. According to

final, 2016, accessed July 14, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

[43] European Commission, "Next steps against fake news: Commission sets up High-Level Expert Group and launches public consultation," 2017, accessed July 17, 2018, http://europa.eu/rapid/press-release_IP-17-4481_en.htm.

the Report, a better understanding of the phenomenon is necessary before the elaboration of a comprehensive response.[44]

In its next chapter, the report evaluates measures already developed by relevant actors in the field such as online platforms as well as by press institutions and radio emitters, which strengthened their capacity to verify information, either through the creation of specially dedicated offices or through establishing a cooperation with fact-checking NGOs. Furthermore, campaigns to increase critical thinking and media literacy have been undertaken.[45]

The Report of the High Level Expert Group was followed by the issuing, in 2018, of a Communication on Tackling Online Disinformation[46] and the adoption of a Code of Conduct for online providers.[47] After defining the concepts of disinformation and categorizing its main ways of spreading, the Communication presents four main principles which lie at the heart of the action against disinformation. These are transparency, defined as a better knowledge of the source of information, and the way it is sponsored and disseminated, diversity of information, understood as increasing the number of the sources of information available to the public, credibility understood as flagging false information to deter its spread and inclusiveness, defined as employing long-term solutions that involve a wide number of stakeholders.

The Communication foresees the elaboration of a EU-wide code of conduct for online platforms, which would require them to better scrutinize the way advertising is paid for and to better identify and close fake accounts, as well as to improve users' ability to access a diversity of verified information. Further, through the Communication, the Commission foresees a stronger cooperation with fact-checkers, better cyber-security tools to more easily identify the source of a particular piece of information online, an increase in research oriented to new technologies that help with the identification of false information, a better coordination between national authorities responsible with election management in order to prepare for the 2019 European Elections, the improvement of media literacy, including through the formation of an Expert

[44] European Commission and authors, "A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation," 2018, accessed July 13, 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

[45] European Commission and authors, "A multi-dimensional approach," 18.

[46] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling online disinformation: a European Approach," 2018, accessed July 13, 2019, https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX 52018DC0236&from=EN.

[47] European Commission, "Code of Practice on Disinformation," 2018, accessed July 13, 2019, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

Group and the funding of related projects through Erasmus+ and the support of quality journalism.[48]

The Code of Conduct for online platforms was issued in 2018 and includes a set of actions that the signatories commit to, which include limiting the possibilities of fake commercial advertising, implementing policies for the transparency of the sources of funding for political advertising, including single-issue advertising, the identification and banning of automated bots and investing in technologies that increase the diversity and the quality of information available to consumers.[49]

## Data Analysis

As can be seen in Table 2, from the twenty-two policy actions which the European Union adopted in order to combat hybrid warfare, ten were classified as “political” and twelve as “technical”. This classification was done based on the nature of the policy field: if a certain policy implied only issues that involved increased cooperation between technical authorities, or between expert groups, or involved the improvement of technical capabilities of specific authorities. Alternatively, policy were classified as “political” when they involved the affirmation of identity or the investment in military equipment or an affirmation of the values and identity which the European Union desires to project.

Considering the actual policies that the EU institutions adopted, eight could be classified as the coordination of inter-governmental cooperation, thirteen as action by supra-national institution which did not involve the adoption of legislation (while not counted, all the actions performed in the struggle against disinformation can also be included here), seven new pieces of supra-national legislation were elaborated or adopted and three CFSP/CSDP actions were adopted or envisioned.

Action by supra-national institutions through their internal capabilities represented the main policy tools in both the political and the technical areas. However, the main difference identified is that in the “political” fields, which mostly involved CFSP/CSDP actions, the lead institution was the High Representative while in the "technical" fields, actions are mostly driven by the

[48] European Commission, “Tackling online disinformation.”

[49] European Commission, “Code of Practice on Disinformation, European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. Joint Communication to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions Report on the implementation of the Action Plan Against Disinformation,” 2019, accessed July 14, 2019, https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52019JC0012&from=EN.

Commission. Furthermore, given that many more "technical" fields fall within the scope of the EU's internal action, a greater number of legislation was adopted. One notable exception, which was coded as a "political" field are policy actions to combat radicalization, where a directive is being considered. Between the two types of fields, the same number of policy actions rely on the coordination of inter-governmental cooperation.

Overall, the data provides a cautious support for the rational choice institutionalist approach, given that considerably more legislation and internal actions (even if one includes the CFSP decisions adopted through inter-governmental means under the broad concept of "legislation") have been adopted in "technical" rather than "political" fields. This would support the claim that EU institutions have a cautious approach to combating hybrid threats and prefer to use this new situation to consolidate policies that had already been planned and which are relatively less controversial. This could also be said about policies adopted to combat disinformation, which include a broad number of stakeholders and which resulted in action which is not based on new legislation. Furthermore, the High Representative was the main "spearhead" in foreign policy. However, it also preferred to use its own resources to establish institutions such as EastStratcom or the Hybrid Fusion Cell, while issues that required a broad cooperation by governments were addressed in inter-governmental formats with the EU taking a more coordinating rather than supra-national role.

Thus, one can argue that the EU institutions are only slowly supra-nationalizing power and are acting to minimize a backlash from the governments of member states. Technical policy fields allow for more support to be built, given that transnational expert networks are more easily built by supra-national institutions. Even in the face of an external threat, the EU acts cautiously to build its own legitimacy and allows political decisions to be made by national governments.

## Conclusion

The article argued that the Russian Federation's new assertiveness has been conceptualized by the institutions of the European Union as "hybrid warfare" and has been addressed through a series of policy tools which are grouped under three main categories: identifying the nature of the threat, improving awareness and building resilience and that an analysis of these policies offers cautious support for rational-choice instiutionalism. Further, the article argued that the EU institutions proceeded cautiously and preferred to adopt supra-national policies in areas where this is bound to cause the least backlash.

Technical policy fields were the preferred area of action of EU institutions, which adopted both legislative acts and coordinated a number of cooperation initiatives in areas which help improve capabilities and information exchange of technical agencies. Alternatively, the EU acted less and less supranationally in traditional areas of state prerogative, such as foreign policy and the identification of vulnerabilities, allowing member states to take the lead and to report on their own state of preparedness.

While not decisive, the data collected for this article provides cautious support for a rational-choice institutionalist approach, which argues that actors seek to minimize risk and maximize benefits and will pursue a "path of least resistance" in pursuing their power interest. Alternatively, data has shown that while the affirmation of "values" is important for the EU, less has been done to concentrate power and more has been allowed to the member states when addressing their own vulnerabilities and handling the relation with the Russian Federation.

# Annexes

***Table 1 : European Union policies to combat hybrid threats 2016-2019***

| **Action** | **Institutional actor entrusted with application of the action.** | **Type of action/ Policy field** | **State of the art in July 2017** | **State of the art in July 2018** | **State of the art in May 2019** |
|---|---|---|---|---|---|
| **Recognizing the Hybrid Nature of a Threat** | | | | | |
| *Member States, supported as appropriate by the Commission and the High Representative, are invited to launch a hybrid risk survey to identify key vulnerabilities, including specific hybrid related indicators, potentially affecting national and pan-European structures and networks.* | Member states supported by the Commission and the HR | Coordination of intergovernmental cooperation<br>Political | The "Friends of Presidency" groups was created (an ad-hoc group established as a preparatory body of the Council of the European Union) and a questionnaire was created and distributed concerning the vulnerabilities of each member state. | Plans were being put forward to prolong the Mandate of the FoP group. | A summary of the findings based on 24 questionnaires was presented during the Bulgarian presidency The Mandate of the "Friends of Presidency" group was extended in June 2018. |
| **Organizing the EU response: improving awareness** | | | | | |
| *Creation of an EU Hybrid Fusion Cell within the existing EU INTCEN structure, capable of receiving and analysing classified and open source information on hybrid threats. Member States are invited to establish National Contact Points on hybrid threats to ensure cooperation and secure communication with the EU* | High Representative and Member States | **Supra-national action - internal (action by the High Representative at the EEAS).** Coordination of inter-governmental cooperation.<br>Political | The cell was created at the level of INTCEN and has begun to distribute analysis, including the Hybrid Bulletin. | The Cell was operational and integrated in the EEEAS. It already participated, by disseminating analysis products during the PACE17 exercises.<br>. | The Cell is operational and several vacancies need to be filled. |

| | | | | | |
|---|---|---|---|---|---|
| *Hybrid Fusion Cell.* | | | | | |
| *The High Representative will explore with Member States ways to update and coordinate capacities to deliver proactive strategic communications and optimise use of media monitoring and linguistic specialists.* | The High Representative<br>Member States | Coordination of inter-governmental cooperation<br>Political | In 2015, the Council of the European Union founded EastStratcom which aims at anticipating disinformation and negative information campaigns. The website euvsdisinfo.eu was released and its associated newsletter which disseminates the results identified to a wider audience. | A new communication was adopted "Tackling online disinformation: a European approach"<br>in April 2018 EastStratcom continued to debunk disinformation from the the Russian-speaking media.<br>Awareness -raising campaigns and cooperation have been undertaken in Eastern Partnership countries. | The *Action Plan against Disinformation* was endorsed by the European Council in December 2018.<br>A Rapid Alert System was set up to enable Member States and EU institutions to facilitate sharing of data, enable common situational awareness, facilitate the development of common responses, and ensure time and resource efficiency. |
| *Member States are invited to consider establishing a Centre of Excellence for 'countering hybrid threats'.* | Member states | Coordination of inter-governmental action<br>Political | The Centre is based on a memorandum of understanding signed on 11.04.2017 by nine countries, which were joined by other three at the end of the year. The Center was launched in Helsinki with HR Mogherini and NATO Secretary General Stoltenberg attending (EEAS 2017) | 16 states have become members of the Helsinki CoE.<br>Three Communities of Interest: on Hybrid Influencing, Vulnerabilities and Resilience and Strategy and Defence. A sub-group on non-state actors has been established | 22 Member States have become Members of the Helsinki CoE.<br>In September 2018, the CoE facilitated a scenario-based discussion at a joint meeting of the Political and Security Committee and the North Atlantic Council, which was broadly appreciated. |
| **Organizing the EU response: building resilience** | | | | | |
| *The Commission, in cooperation with* | The Commission | Supra-national action - internal (the use of the | A workshop on critical | A draft manual of vulnerability indicators and | The list of vulnerability indicators |

| | | | | | |
|---|---|---|---|---|---|
| *Member States and stakeholders, will identify common tools, including indicators, with a view to improve protection and resilience of critical infrastructure against hybrid threats in relevant sectors.* | | European program in order to improve critical infrastructures) A better application of the directive on critical infrastructure<br>Supra-national action - legislation<br>Technical | infrastructures was organized and a roadmap elaborated on future activities. | resilience hybrid threats to critical infrastructures in the EU has been developed.<br>A proposal for a Regulation establishing a framework for screening of foreign direct investments into the European Union if they are likely to affect security or public order has been elaborated. | for the resilience and protection of critical infrastructure against hybrid threats has been completed. The EU adopted Regulation (EU) No 2019/452 [11] setting up a framework for the screening of investments from non-EU countries that may affect security or public order. |
| *The Commission, in cooperation with Member States, will support efforts to diversify energy sources and promote safety and security standards to increase resilience of nuclear infrastructures* | The Commission<br>Member States | Supra-national action -legislation (a directive will be elaborated which is to apply directly to member states)<br>Coordinating inter-governmental cooperation (on gas pipelines)<br>Technical | Legislation was elaborated on ensuring the security of gas supply, which was agreed, in principle, by the Council and the Parliament. | In September 2017, a Joint Communication : “Resilience, Deterrence and Defence: Building strong cybersecurity for the EU” was adopted.<br>*The Commission will continue supporting the European Energy Information Sharing and Analysis Centre on cybersecurity.*<br>Member States are implementing the Security of Gas Supply Regulation.<br>The Risk Preparedness Regulation, is under negotiations. | The European Parliament and the Council reached in November 2018 an agreement on the Commission’s Proposal for Regulation on risk-preparedness in the electricity sector<br>The Commission has been also actively supporting Member States in the implementation of Regulation (EU) 2017/1938 [14] concerning measures to safeguard the security of gas supplies. |
| *The Commission will monitor emerging threats across the transport sector* | The Commission<br>The High Representative<br>Member | Supra-national action (direct action by the Commission through internal | A methodology for the "common | Risk analyses of maritime threats are being undertaken.<br>The Information | Regulation (EU) 2019/123 on the implementation of Air Traffic Network |

| | | | | | |
|---|---|---|---|---|---|
| *and will update legislation where appropriate. In implementing the EU Maritime Security Strategy and the EU Customs Risk Management Strategy and Action Plan, the Commission and the High Representative (within their respective compentences), in coordination with Member States, will examine how to respond to hybrid threats, in particular those concerning transport critical infrastructure*. | States | means).<br>Supra-national legislation<br>Technical | evaluation of risks to be undertaken at the EU level" was elaborated with the help of national air security experts and with the support of the EEAS. This will allow the exchange of classified information and the definition of a common vision on risk. | Sharing Environment is being upgraded. An action plan to improve military mobility through the use of the Trans-European network was being elaborated. | Functions has been adopted. It created the European Aviation Crisis Coordination Cell (ECCC).<br>The EU Maritime Security Strategy Action Plan has been revised. |
| *Within the context of the Space Strategy and European Defence Action Plan, the Commission will propose to increase the resilience of space infrastructure against hybrid threats, in particular, through a possible extension of the Space Surveillance and Tracking scope to cover hybrid threats, the preparation for the next generation of GovSatCom at European level and the introduction of Galileo in critical infrastructures* | The Commission | Supra-national action (direct action by the Commission through its own agencies)<br>Technical | No concrete action, but the issues of resilience will be integrated in future regulation.<br>. | The Commission elaborated a Space Programme of the Union, which includes aspects to increase the resilience of critical infrastructure. | Plans to implement GOVSATCOM - a system of satellite based governmental communications has been elaborated and a draft exercise project has been started.<br>Given that the HR and the Council have responsibilities for the security of space assets, the HR has elaborated hybrid war scenarios which include attacks on the EU's satellites. |

| | | | | | |
|---|---|---|---|---|---|
| *dependant on time synchronisation.* | | | | | |
| *The High Representative, supported as appropriate by Member States, in liaison with the Commission, will propose projects on how to adapt defence capabilities and development of EU relevance, specifically to counter hybrid threats against a Member State or several Member States.* | The High Representative | Inter-governmental adoption of EU policies (the European Defense Agency is coordinated by the HR but is overseen by a board composed of member state representatives)<br>Political | • three table top exercises based on hybrid scenarios<br>• The inclusion of the hybrid dimension in the 2005 Requirements Catalogue<br>• analysis report on military implications stemming from hybrid attacks directed against critical harbor infrastructure | The Commission proposed in a Regulation establishing a European Defence Industrial Development Programme. A provisional agreement on the draft Regulation was reached on 22 May 2018 by the European Parliament and the Council. For the next EU Multiannual Financial Framework, the Commission proposed an integrated European Defence Fund with an ambitious budget of EUR 13 billion. | The Council and the European Parliament reached a partial agreement on the Proposal for Regulation establishing the European Defence Fund for the 2021-2027 Multiannual Financial Framework<br>. |
| *The Commission, in cooperation with Member States, will improve awareness of and resilience to hybrid threats within existing preparedness and coordination mechanisms, notably the Health Security Committee.* | The Commission Member States | Supra-national action (internal to EU institutions)<br>Coordinating inter-governmental cooperation<br>Technical | • An exercise was planned for the autumn of 2017, concerning hybrid and multi-dimensional threats<br>• A common action on vaccination, including the predictions concerning the supply and demand of vaccines and the research on vaccines<br>• Creation of a network of funders of health | The Commission organized Chimera, an exercise for the health, civil protection and security sectors throughout the EU and third countries to test preparedness and response planning to serious cross-border threats.<br>.<br>In April 2018, the Commission published a Communication and submitted a proposal for a Council Recommendation to strengthen the EU cooperation against vaccine- | The report on the Chimera exercise was adopted.<br>A workshop was organized in April 2019, in cooperation with the US Federal Bureau of Investigation (FBI) and the US Centres for Disease Control and Prevention (CDC),<br>Decision (EU) 2019/420 of the European Parliament and of the Council of 13 March 2019 has been adopted. |

| | | | | | |
|---|---|---|---|---|---|
| | | | research abroad | preventable diseases. | |
| *The Commission encourages Member States as a matter of priority to establish and fully utilise a network between the 28 CSIRTs and the CERT-EU (Computer Emergency Response Team-EU) as well as a framework for strategic cooperation. The Commission, in coordination with Member States, should ensure that sectorial initiatives on cyber threats (e.g. aviation, energy, maritime) are consistent with cross-sectorial capabilities covered by the NIS Directive to pool information, expertise and rapid responses.* | The Commission | Supra-national - internal (applying the NIS directive)<br>Supra-national action- legislation<br>Coordinating inter-governmental cooperation.<br>Technical | • Adopting the NIS directive in 2017<br>• Expansion of the mandate of the ENISA and its transformation in the EU cyber-security agency<br>• A European framework for certifying the security of cyber-products.<br>• The funding of cyber defense projects through PESCO (suggested in September 2017 through the State of the Union Address) | The European Defense Agency organized CYBRID 17, a cyber response incident exercise.<br>The Commission monitors the way in which the NIS directive is adopted. | A network of Computer Security Incidents Response Teams has been established and work is progressing on building trust between its members and with CERT-EU.<br>The Commission adopted a Proposal for Regulation to establish the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centers.<br>A Cybersecurity Act was adopted on 17 April 2019 |
| *The Commission, in coordination with Member States, will work together with industry within the context of a contractual Public Private Partnership for cybersecurity, to develop and test technologies to better protect users and infrastructures against cyber aspects of hybrid threats.* | The Commission | Supra-national action (independent action by the Commission)<br>Technical | • The signing, by the Commission, of a public-private partnership for cyber-security | The Commission signed a public-private partnership on cybersecurity with the European Cybersecurity Organisation (ECSO).<br>The *Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity in Europe* was adopted. | A European Cybersecurity Industrial, Technology and Research Competence Centre is being planned. |
| *The Commission will issue guidance to* | The Commission | Supra-national action (independent | Planning a sectoral strategy on | The Commission will establish an | In April 2019, the Commission adopted a |

| | | | | | |
|---|---|---|---|---|---|
| *smart grid asset owners to improve cybersecurity of their installations. In the context of the electricity market design initiative, the Commission will consider proposing 'risk preparedness plans' and procedural rules for sharing information and ensuring solidarity across Member States in times of crisis, including rules on how to prevent and mitigate cyber-attacks.* | | action by the Commission)<br>Technical | cyber-security in the field of energy (where smart networks have appeared) | energy sectoral work stream under the NIS Cooperation Group to address the particularities of the energy sector and to provide guidance to Member States on the implementation of the NIS Directive | Recommendation on cybersecurity in the energy sector. |
| *The Commission, in cooperation with ENISA, Member States, relevant international, European and national authorities and financial institutions, will promote and facilitate threat information-sharing platforms and networks and address factors that hinder the exchange of such information.* | The Commission | Supra-national action (elaborating a legislative framework applicable to all member states and Commission's independent action)<br>Technical | • Modifying the Directive on Payment Services<br>• Elaborating minimal technical standards on the strict authentication of clients and the secure communication of payments. | The Fintech action plan was elaborated. to eliminate barriers that limit information exchange between market players. | . |
| *The Commission and the High Representative (within their respective areas of competence), in coordination with Member States, will* | The Commission The High Representative | Supra-national action (internal action of supra-national institutions)<br>Technical | • Elaborating the common research agenda of the commission and the | CERT-EU has signed a Service Level Agreement with EUROCONTROL and a Memorandum of Cooperation with the | The the European Aviation Safety Agency (EASA) is s currently developing the European Centre for Cyber Security |

| | | | | | |
|---|---|---|---|---|---|
| *examine how to respond to hybrid threats, in particular those concerning cyber-attacks across the transport sector*. | | | EEAS<br>• The capacity to handle hybrid threats by national authorities with coastguard functions was analyzed and measures to increase cooperation were suggested | European Aviation Safety Agency | in Aviation (ECCSA), which is currently in its pilot phase.<br>The Commission is working on transposition of the new International Civil Aviation Organization (ICAO) cybersecurity standard to the Aviation Security Implementing Regulation.<br>Implementation of EU Maritime Security Strategy Action Plan concerning preparedness and response to hybrid threats, in particular to cyber attacks across the transport sector in ongoing. |
| *The Commission will use the implementation of the Action Plan on Terrorist Financing to also contribute to countering hybrid threats.* | The Commission | Supra-national action - legislation (the elaboration of a supra-national framework, the elaboration of implementation standards).<br>Technical | • three legislative proposals on the introduction of criminal sanctions in the case of money laundering and illicit cash payments, concerning the freezing of assets and the confiscation of goods<br>• the monitoring of the transposition of the fourth Directive on the | A proposal for a Directive was launched to to step up the cooperation between the authorities responsible for combating serious crime and terrorism and to enhance their access to and use of financial information.<br>The 5th Anti-Money Laundering Directive was adopted. | The implementation of the 5th anti-money laundering directive is ongoing. |

| | | | | | |
|---|---|---|---|---|---|
| | | | combating of money laundering.<br>• a legislative proposal to consolidate the directive with supplementary measures.<br>• a regulation proposal with the aim of preventing the import and the storage in the EU of cultural assets illegally exported from other countries. | | |
| *The Commission is implementing the actions against radicalisation set out in the European Agenda on Security and is analysing the need to reinforce procedures for removing illegal content, calling on intermediaries' due diligence in managing networks and systems.* | The Commission | Supra-national action (internal action of supra-national institutions);<br>**Adoption of supra-national legislation**<br>Political | • The development of the Radicalization Awareness Network.<br>• Developing the EU Internet Referral Unit at Europol, and the EU Internet Forum<br>• Elaborating a code of Conduct for countering illegal hate speech online | The Commission has launched an impact assessment to determine whether current efforts are sufficient or whether additional measures are needed. | The Commission adopted a Proposal for Regulation to prevent the dissemination of terrorist content online.<br>The European Strategic Communications Networks working on the issue of disinformation and its implications. |
| *The High Representative,* | The High Representative | Supra-national action (internal | • a study on risks | Dedicated Hybrid Risk | Hybrid Risk Surveys have been |

| | | | | | |
|---|---|---|---|---|---|
| *in coordination with the Commission, will launch a hybrid risk survey in neighborhood regions. The High Representative, the Commission and Member States will use the instruments at their respective disposal to build partners' capacities and strengthen their resilience to hybrid threats. CSDP missions could be deployed, independently or to complement EU instruments, to assist partners in enhancing their capacities.* | The Commission | action of supra-national institution) **Inter-governmental adoption of EU policies (a possible CSDP mission).**<br>Political | elaborated in the framework of a pilot-project developed together with the Republic of Moldova with the aim of identifying the country's main vulnerabilities and to ensure that the EU targets the specific fields<br>• further recommendations on the basis of this research.<br>• Program on the cyber resilience of third countries. | Surveys are being launched to identify the critical vulnerabilities and provide targeted support for EaP countries. These surveys have been used in Republic of Moldova. In 2018, Jordan and Georgia have officially requested the EU to undergo vulnerability surveys. | launched in seven partners: Moldova, Georgia, Jordan, Albania, North Macedonia, Kosovo and Montenegro. |
| **Preventing, responding to crisis and recovering** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| *The High Representative and the Commission, in coordination with the Member States, will establish a common operational protocol and carry out regular exercises to improve strategic decision-making capacity in response to complex hybrid threats building on the Crisis Management and Integrated Political Crisis Response procedures.* | The High Representative<br>The Commission<br>The Member States | Supra-national action (internal action of supra-national institutions)<br>The coordination of inter-governmental cooperation<br><br>Technical | • The elaboration of the EU's operational protocol on the combating of hybrid threats (EU playbook).<br>• Improving the synergy with NATO, which has elaborated a protocol on the cooperation of the EU.<br>• Coordinating the decision-making procedure between the two institutions. | A EU operational protocol has been established and tested during the 2017 NATO-EU Parallel exercises. NATO-EU interaction has been greatly expanded. | The EU Hybrid Exercise MULTILAYER 18 - EU HEX-ML 18 (PACE)<br>Has been carried out on the basis of the Playbook. |
| *The Commission and the High Representative, in their respective areas of competence, will examine the applicability and practical implications of Articles 222 TFEU and Article 42(7) TEU in case a wide-ranging and serious hybrid attack occurs.* | The Commission<br>The High Representative | Supra-national action (internal action of supra-national institutions)<br><br>Political | When joint exercises are organized, of the invocation of the solidarity clause by a state. | | |
| *The High Representative, in coordination with Member States, will integrate, exploit and coordinate the capabilities of military action in countering hybrid threats within the Common Security and* | The High Representative | **Supra-national action (internal action of supra-national institutions)**<br><br>Political | Elaborating a document called *EU military contribution to countering hybrid threats within the CSDP.* | The "EU military contribution to countering hybrid threats within the Common Security and Defence Policy" plan has been finalized. The Concept Implementation Plan is being elaborated. | The "EU Concept for EU-led Military Operations and Missions" is being modified to out to include hybrid threats aspects. |

| | | | | | |
|---|---|---|---|---|---|
| *Defence Policy* | | | | | |
| *The High Representative, in coordination with the Commission, will continue informal dialogue and enhance cooperation and coordination with NATO on situational awareness, strategic communications, cybersecurity and "crisis prevention and response" to counter hybrid threats, respecting the principles of inclusiveness and autonomy of each organisation's decision making process.* | The High Representative<br>The Commission | **The inter-governmental adoption of EU policies (the Warsaw** NATO-EU declaration was adopted by the European Council)<br><br>Political | A set of 42 proposals was elaborated and it was, subsequently endorsed in separate, parallel processes on 6 December 2016 by both the EU and NATO Councils**.**<br><br>**The first exchanges were carried out between the NATO Hybrid Analysis Cell and the EU Hybrid Fusion Cell.**<br><br>. | The PACE17 exercise has tested the two organisations' 'Playbooks' and, through that, their capacity to work together to support their members.<br><br>Consultations on Strategic Communication have taken place support for Ukraine, Bosnia and Herzegovina, the Republic of Moldova and Georgia. | The PACE 2018 exercise has deepened the lessons from PACE 2017. PACE 2018 was based on a hybrid scenario including cyber-security, disinformation and civil protection.<br><br>Staff-to-staff meetings on cyber-security, CBRN and situational awareness. |

*Source:* This table was constructed through analyzing the following documents: European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint communication to the European Parliament and the Council: 'Joint Framework on countering hybrid threats - a European Union response'," JOIN(2016) 18 final, 2016, accessed July 14, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018 &from=EN; European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats - a European Union response," 2017, accessed July 14, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=CELEX:52017JC0030&from=GA; European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Joint Report on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018," 2018, accessed July 14, 2019, https://eeas.europa.eu/sites/eeas/files/joint_report_on_the_implementation_of_the_joint_frame work_on_countering_hybrid_threats_from_july_2017_to_june_2018.pdf; European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 2019 "Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats," 2019, accessed July 14, 2019, https://eeas.europa.eu/sites/eeas/files/report_on_the_ implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joi nt_communication_on_increasing_resilien.pdf; European Union and NATO, "Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization," 2016, accessed June 13, 2019, https://www.nato.int/cps/de/natohq/official_texts_133163.htm; European Union and NATO, "Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016," 2017, accessed June 13, 2018, https://eeas.europa.eu/

sites/eeas/files/170614-joint-progress-report-eu-nato-en-1.pdf; European Union and NATO,"Second progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016," 2017, accessed July 2, 2019, http://www.consilium.europa.eu/media/35577/report-ue-nato-layout-en.pdf; European Union and NATO, "Third progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017," 2018, accessed June 13, 2018, http://www.consilium.europa.eu/media/35578/third-report-ue-nato-layout-en.pdf.

***Table 2 - Synthetic analysis of European Policies for combating hybrid threats***

| **Field** | **Type of action** |
|---|---|
| Political (10 fields) | 4 Coordination of inter-governmental cooperation<br>5 Supra-national action - internal<br>1 Supra-national action - legislation<br>3 Inter-governmental adoption of EU policies |
| Technical (12 fields) | 4 Coordination of inter-governmental cooperation<br>9 Supra-national action - internal<br>6 Supra-national action - legislation |