УДК 32.019.51, 327.8

Дарья БАЗАРКИНА

ЭВОЛЮЦИЯ ПОДХОДОВ К ПРОТИВОДЕЙСТВИЮ ГИБРИДНЫМ УГРОЗАМ В СТРАТЕГИЧЕСКОМ ПЛАНИРОВАНИИ ЕС

Статья поступила в редакцию 13.10.2021

Аннотация. В статье выявлены основные компоненты подхода ЕС к противодействию гибридным угрозам. Автор пришел к выводу, что «открытая архитектура» теории гибридной войны, широкие возможности трактовки определения гибридных угроз позволяют совершенствовать практические меры и теоретический подход к проблемам безопасности. Однако на фоне углубления экономической конкуренции и политических противоречий между государственными акторами подход к противодействию гибридным угрозам гиперполитизируют и используют для оправдания санкционного давления, усиления военных блоков или массированных информационных кампаний против политического оппонента. ЕС формирует и совершенствует системный подход к обеспечению безопасности в условиях роста гибридных угроз. Однако экономическое соперничество и разногласия стран Запада с Россией и Китаем создают политическую конъюнктуру, при которой последних постоянно обвиняют в создании гибридных угроз для ЕС. Чрезмерное употребление риторики теории гибридной войны в дискурсе ЕС ставит под удар безопасность Европы.

Ключевые слова: гибридные угрозы, теория гибридной войны, стратегическое планирование, Комиссия ЕС, Европейский парламент, Европейская внешнеполитическая служба.

Общие потребности государств и граждан в эпоху «информационных и физических вирусов» создают реальную основу для сотрудничества [Lunkin, 2021: 19], однако в Европе ему мешает негативная атмосфера в отношениях России и ЕС. При сохранении существующих тенденций в сфере информационной безопасности последовательное формирование репутации России как источника гибридных угроз способно со временем легитимизировать в глазах общественности в Европе самое жесткое давление на РФ, вплоть до создания военной опасности, и свести на нет

© Базаркина Дарья Юрьевна – д.полит.н., ведущий научный сотрудник, Отдел исследований европейской интеграции, Институт Европы Российской академии наук.

Адрес: Российская Федерация, 125009, г. Москва, ул. Моховая, д. 11, стр. 3.

E-mail: bazarkina-icspsc@yandex.ru

DOI: <http://dx.doi.org/10.15211/soveurope62021133143>

попытки наладить перспективный диалог. Это делает актуальным анализ европейского подхода к борьбе с гибридными угрозами.

В настоящей статье, опираясь на положения теории гибридной войны, предпринята попытка выявить основные компоненты подхода ЕС к противодействию гибридным угрозам, обозначенным в документах стратегического планирования Союза. Для этого были поставлены исследовательские вопросы: 1) Как определяет гибридные угрозы теория гибридной войны, каковы ее сильные и слабые стороны? 2) Как подход к борьбе с гибридными угрозами регламентируется в ЕС? 3) Какие изменения происходят в этом подходе под влиянием тенденций последних лет, в том числе кризиса, вызванного коронавирусной пандемией?

Определение гибридных угроз в теории гибридной войны

ЕС и его государства-члены начали активно использовать термин «гибридная война» в ходе украинского конфликта [Krivko and Bolgov, 2021: 257; Kraft, 2018: 309]. 18 сентября 2014 г. Европейский парламент «решительно осудил» Россию «за ведение необъявленной “гибридной войны” против Украины»¹.

Под гибридной войной первоначально понимали «силовые конфликты, где используют различные формы и методы ведения вооруженной и невооруженной борьбы». Имеются в виду информационные и кибероперации, развертывание и применение сил специального назначения, сочетание регулярных и повстанческих сил и т. д. [Krivko and Bolgov, 2021: 257]. Создатель теории гибридной войны Ф. Хоффман подчеркивал, что такие войны могут вестись как негосударственными субъектами, так и государствами [Hoffman, 2009: 38]. Понятие постепенно распространяется на конфликты, в которых открытое применение силы противниками может начаться только на заключительном этапе [Герасимов, 2013] после применения политических, экономических, информационных и других невоенных мер.

Ф. Хоффман определяет гибридные угрозы [Hoffman, 2010: 443] как исходящие от «любого противника, который одновременно и адаптивно использует сочетание обычных вооружений, нерегулярной тактики, терроризма и преступного поведения в боевом пространстве для достижения политических целей». НАТО расширяет определение до «угроз, создаваемых противниками, способными одновременно адаптивно использовать традиционные и нетрадиционные средства для достижения своих целей»², что позволяет постепенно включать в перечни гибридных угроз формы экономического противоборства, психологические операции [Cusumano and Corbe, 2018: 5] и другие действия.

¹ Situation in Ukraine and state of play of EU-Russia relations. European Parliament resolution of 18 September 2014 (2014/2841(RSP)). URL: https://www.europarl.europa.eu/doceo/document/TA-8-2014-0025_EN.html (дата обращения: 23.09.2021)

² NATO Allied Command Transformation, 2010. Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats. 25 August. URL: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf (дата обращения: 23.09.2021)

Теория гибридной войны и связанные с ней подходы встречают критику в исследовательских кругах. Особенно значимой для формирования теоретической базы статьи стала оценка Г. Саймонса [Simons, 2021], который считает данную теорию «весьма спорной, в немалой степени из-за очень высокого уровня политизации» (что ведет к приписыванию гибридных действий «другим», но не «нам»), а также отмечает расплывчатость теории, что позволяет заинтересованным политическим акторам манипулировать различными сторонами в конфликте, «например, создать вооруженный конфликт, где нападающий может быть воспринят как жертва» [Simons, 2021: 6]. Меры имплементации теории гибридной войны часто имеют негативные последствия. Так, санкции «часто вызывают сильные эмоции», затрудняя поиск разумной стратегии и провоцируя лишь контрсанкции [Biscop, 2021: 2]. В западном академическом дискурсе выявлены устойчивые попытки связать акт гибридной войны с действиями экономических конкурентов и политических оппонентов, главным образом Китая, Ирана и России [Панцеров, 2020]. На такой основе политическая сила, сообщающая о гибридной угрозе, может создать впечатление о чрезвычайной ситуации в международных отношениях для проведения агрессивной внешней политики под видом обороны [Simons, 2021: 6].

Учитывая, что теория гибридной войны изначально предполагает наличие у противника политической цели [Rinelli, Duyvesteyn, 2018: 20], политизация оценок гибридных угроз неизбежна. Однако чрезмерная политизация ведет к переносу военной риторики на процессы, происходящие в мирное время (отсюда гибридные угрозы все чаще называют без упоминаний собственно гибридной войны, гибридного противоборства и т. п.). Любые действия конкурента или оппонента преподносятся как гибридные, следовательно, как подготовка к военным действиям (в том числе конкурентная борьба за рынки сбыта). Это несет выгоду стороне, которая первой выступит с обвинениями, если она имеет материальные и технические ресурсы для доминирования в глобальном информационном поле.

Основные положения подхода ЕС в области борьбы с гибридными угрозами

Европейская внешнеполитическая служба (ЕВС) определяет гибридные угрозы как сочетание традиционных и нетрадиционных, военных и невоенных действий, координируемых государственными или негосударственными субъектами, ставящими определенные политические цели¹. В их число входят кибератаки, нарушения функционирования критически важных услуг (поставка энергоносителей или обеспечение финансовых операций), подрыв общественного доверия к правительственным учреждениям или углубление социальных противоречий, а также использование химических, биологических, радиационных или ядерных веществ, доставленных нетрадиционным способом. Такой подход формировался по мере того, как в повестку дня ЕС включались вопросы экономической и политической конкуренции. Приведенный ни-

¹ European External Action Service, 2021. Безопасная Европа: Противодействие гибридным угрозам. URL: https://eeas.europa.eu/headquarters/headquarters-homepage_ru/46536/Безопасная-Европа:Противодействие-гибридным-угрозам (дата обращения: 23.09.2021)

же анализ ключевых профильных стратегических документов Евросоюза выявил постепенное расширение военной риторики в разногласиях мирного времени.

Изначально разработка политических мер реагирования на гибридные угрозы началась в 2016 г. в связи с украинским кризисом и событиями в Ливии и Сирии [Giumelli, Cusumano and Besana, 2018: 147; Morillas, 2019: 135] (позже к ним добавятся торговые войны США с Китаем и Россией, в которых у ЕС не получится остаться в стороне). Еврокомиссия и ЕВС обнародовали ряд документов, среди которых особое место занимает Совместная рамочная программа по противодействию гибридным угрозам от 6 апреля 2016 г. (Программа 2016 г.)¹, где наглядно отражена тенденция к секьюритизации общественной жизни, проявившаяся в стратегическом планировании многих стран (борьба с гибридными угрозами в программе представлена как сочетание целого ряда стратегий ЕС – в области энергетической, кибербезопасности, безопасности на море и т. п.).

Несмотря на то что, согласно Совместной рамочной программе 2016 г., источниками гибридных угроз могут быть как государственные, так и негосударственные субъекты, Комиссия и ЕВС концентрируют внимание, прежде всего, на действиях преступных, в том числе террористических групп. Бороться с финансированием гибридных кампаний предлагается в соответствии с Планом действий Евросоюза по борьбе с терроризмом, а защита от них в интернете включает противодействие вербовке террористов.

Это можно связать как с появлением «Исламского государства» (террористическая организация, запрещенная в России), так и с ростом ультраправых настроений и евроскептицизма на фоне миграционного кризиса, охватившего Европу вследствие вооруженных конфликтов на Ближнем Востоке. Одновременно ЕС избегает открытой политической риторики в документе, который регулирует сотрудничество с третьими странами (часть которых поддерживает партнерские отношения с оппонентами Союза). Примечательно, что слово «противоборство» (“warfare”) встречается в Программе 2016 г. всего один раз (для характеристики уровня гибридных угроз «ниже порога официально объявленной войны»), а слово «война» (“war”) – ни разу. В то же время на первый план выходит информационно-психологический компонент (кампании дезинформации с использованием социальных сетей) как средство создания гибридных угроз.

В Программе 2016 г., где обозначены четыре опоры борьбы с гибридными угрозами (осведомленность, устойчивость, кризисное управление и сотрудничество с НАТО), ЕС демонстрирует комплексный подход к обеспечению безопасности на фоне гибридизации международных процессов, что считается преимуществом. Вместе с тем в Программе 2016 г. проявляется политизированность, прежде всего, в аспектах осведомленности (информационно-психологическая безопасность) и совместных с

---

¹ European Commission and European External Action Service, 2016. Joint Framework on countering hybrid threats: a European Union response (Joint Communication to the European Parliament and the Council). JOIN/2016/018 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018&qid=1632230335463> (дата обращения: 23.09.2021)

НАТО инициатив. На пересечении этих двух направлений происходит первый этап развития профильных структур Союза.

Наряду с Подразделением анализа гибридных угроз в составе Центра анализа разведанных ЕС (Интсен), отдельно для работы в информационной сфере Брюссель развивает стратегическую коммуникацию, одна из структур которой (Восточная оперативная рабочая группа) с начала украинского конфликта выполняла функцию «разоблачения» в странах Восточного партнерства «дезинформации, исходящей из прокремлевских источников»¹. Согласно Программе 2016 г., в полной мере используя традиционные СМИ и социальные сети, ЕВС с опорой на Восточную и Арабскую группы стратегических коммуникаций, должна целенаправленно реагировать на дезинформацию. Центр передового опыта по борьбе с гибридными угрозами был открыт в 2017 г. в Хельсинки совместно с НАТО, что можно расценить как дополнительный фактор политизации подхода ЕС в обмен на поддержку военного блока.

Если Комиссия и ЕВС на начальном этапе формирования подхода к борьбе с гибридными угрозами преподносили их даже в отрыве от первоначальной теории гибридной войны, то Европейский парламент в резолюции от 23 ноября 2016 г. прямо обозначает Россию как «актора, ведущего гибридную войну (“hybrid war”) на Донбассе и стремящегося с помощью пропаганды подорвать согласованность внешней политики ЕС»². Россию обвиняли в поддержке антиевропейских сил в ЕС, в частности, «крайне правых партий, популистских сил и движений». Одним из поводов для таких обвинений стала поддержка, оказанная РФ французскому «Национальному объединению» (лидер партии Марин Ле Пен ранее заявляла, что признает итоги референдума в Крыму). Таким образом, политический оппонент постепенно занимает в дискурсе Евросоюза место практически главного источника гибридных угроз.

13 июня 2018 г. Комиссия и высокий представитель ЕС по иностранным делам и политике безопасности опубликовали Совместное сообщение «Повышение устойчивости ЕС и расширение возможностей противодействия гибридным угрозам»³. В этом документе прямо не называется противник (и всего один раз используется слово “warfare”), но в качестве актуального примера гибридной операции приведено отравление Сергея и Юлии Скрипалей в Солсбери. Ранее Европейский Совет в своем заключении от 22 марта 2018 г. согласился с версией британских властей, по которой «*весьма вероятно*, что Российская Федерация несет

¹ European External Action Service, 2021. Questions and Answers about the East StratCom Task Force. URL: <https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-> (дата обращения: 23.09.2021)

² European Parliament, 2016. Resolution of 23 November on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)). URL: https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html (дата обращения: 23.09.2021)

³ European Commission, Secretariat-General, 2018. Increasing resilience and bolstering capabilities to address hybrid threats (Joint Communication to the European Parliament, The European Council and the Council). JOIN/2018/16 final. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52018JC0016> (дата обращения: 23.09.2021)

ответственность» за инцидент¹, и июньское сообщение стало ответом на заявление Совета.

В отличие от программы 2016 г., где террористическая угроза признавалась одной из гибридных угроз, в Сообщении терроризм и гибридные угрозы разделены: говорится о «химических, биологических, радиологических и ядерных угрозах, выходящих за рамки гибридных угроз и охватывающих также террористические угрозы», в чем прослеживается политический интерес – выделить в качестве источника гибридной угрозы, прежде всего, действия государств. Предлагается развитие связей ЕС с профильными региональными центрами передового опыта, в том числе с Североатлантическим альянсом. Вводится новое направление контрмер – борьба с враждебной разведывательной деятельностью. На этом фоне Евросоюз стремится выработать скоординированные с НАТО механизмы гибридного противоборства, которые (если возвратиться к теории гибридной войны) в будущем могут включить и военные меры.

Подход ЕС к борьбе с гибридными угрозами в условиях коронавирусной пандемии

24 июля 2020 г. Комиссия представила новую Стратегию Союза безопасности (ССБ) ЕС², разработка которой «проходила в условиях возрастания значения цифровой среды, в частности, искусственного интеллекта, особенно в период противодействия последствиям пандемии коронавируса» [Потемкина, 2020: 6]. Одновременно с ССБ был обнародован Отчет 2020 г. об имплементации уже упомянутых Совместной рамочной программы 2016 г. и Совместного сообщения 2018 г.³ Влияние глобального кризиса отразилось на системе стратегических приоритетов ЕС, что заметно при сравнении ССБ и Отчета. Последний построен в полном соответствии со структурой Программы 2016 г. и отражает принятые меры по намеченным в ней направлениям (в соответствии с чем, к примеру, защита критической инфраструктуры, борьба с киберпреступностью – направления борьбы с гибридными угрозами). В ССБ 2020 г. упомянуто стирание границ между физическим и цифровым воздействием, нацеленность на уязвимые группы общества, трудность определения источников угроз. Однако гибридные угрозы вынесены в особый параграф, где отделены от киберпреступности или распространения нелегального контента.

¹ European Council, 2018, Conclusions on the Salisbury attack, 22 March 2018. URL: <https://www.consilium.europa.eu/en/press/press-releases/2018/03/22/european-council-conclusions-on-the-salisbury-attack/> (дата обращения: 23.09.2021)

² European Commission, Secretariat-General, 2020. On the EU Security Union Strategy. COM/2020/605 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605> (дата обращения: 23.09.2021)

³ Council of the EU, 2020. Report on the implementation of the 2016 Joint Framework on counter-ing hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats. SWD (2020) 153. URL: <https://data.consilium.europa.eu/doc/document/ST-10047-2020-INIT/en/pdf> (дата обращения: 23.09.2021)

По сути, два документа дублируют стратегию безопасности. Ключевое отличие Отчета от ССБ – повышенное внимание к борьбе с дезинформацией и иностранной пропагандой. ССБ, в свою очередь, стал результатом осмысления реального глобального кризиса. Политизированность оценок хотя и присутствует в ней, отходит на второй план перед общими для всего мира угрозами. Многие меры противодействия гибридным угрозам, представленные в Отчете (диверсификация поставок энергоносителей, разработка и внедрение в ЕС собственных систем спутниковой связи и т. п.), могут быть и мерами имплементации ССБ.

ССБ акцентирует внимание на последствиях коронавирусной пандемии, в частности, на росте организованной преступности, киберпреступности, угрозах злонамеренного использования искусственного интеллекта. Комиссия связывает эти явления с гибридизацией международных отношений («напористая промышленная политика третьих стран в сочетании с продолжающимся хищением интеллектуальной собственности киберпреступниками меняет стратегическую парадигму защиты... европейских интересов»¹). Однако, в отличие от документов, принятых до пандемии, в которых акцент делался прежде всего на политических целях предполагаемого противника, подход в новой ССБ представляется более взвешенным: социальные разногласия на фоне стремительного развития цифровой среды выходят на первый план как факторы гибридных атак.

ССБ 2020 г. можно назвать попыткой Комиссии временно пересмотреть подход к противодействию гибридным угрозам в условиях мирового кризиса. Однако и она не свободна от политизированных оценок, заданных рамками теории гибридной войны и стратегическими документами 2016–2018 гг. Международное сотрудничество ЕС в области безопасности развивается прежде всего с НАТО и его союзниками. Стремление же преодолеть разногласия с Россией (и Китаем, которому уделяется особое внимание в рамках борьбы с дезинформацией) в список приоритетов Евросоюза не вошло даже на фоне того, что пандемия, сопровождающаяся прекращением поставок важных комплектующих, в основном из КНР, привела экономики европейских стран, особенно сектор услуг, на грань коллапса [Белов, 2021: 60]. Попытки более прагматично подойти к отношениям с этими странами встречаются в ЕС активное сопротивление атлантистов (примером можно назвать острую критику позиции Ж. Борреля в Европарламенте после его визита в Москву [Данилов, 2021: 8]).

Если на первых этапах формирования подхода Брюсселя к борьбе с гибридными угрозами основным фактором его гиперполитизации выступал украинский кризис, то в 2020–2021 гг. на первый план выходит торговая война между США и Китаем. В «напористой промышленной политике» все чаще будут обвинять КНР (в основном в связи с ростом влияния компании Huawei на европейских рынках). На отношения России и ЕС также влияют стратегические интересы Вашингтона. Последние ищут способы увеличить долю своей торговли во всем мире, в том числе и на сырьевых рынках ЕС, для чего ускорили добычу сланцевого газа. На этом фоне

---

¹ European Commission, Secretariat-General, 2020. On the EU Security Union Strategy. COM/2020/605 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605> (дата обращения: 23.09.2021)

очевидно стремление элиты США приостановить или отложить запуск проекта «Северный поток-2», который значительно увеличит доступ российского газа на рынок ЕС. Зависимость Евросоюза от импорта сырья для США становится средством давления на европейские власти [Bazarkina, Gramar, 2020: 166–167]. Данный конфликт интересов не мог не повлиять на постепенное включение проблем экономической безопасности в перечни гибридных угроз в Евросоюзе.

План действий в области демократии, обнародованный 3 декабря 2020 г., затрагивает информационно-психологический аспект гибридных войн с особым вниманием к иностранным государственным акторам. В этом документе Комиссия прямо обвиняет Россию и Китай в «дезинформации на фоне пандемии в целях подорвать демократические дебаты и улучшить собственный имидж»¹. В условиях роста общемировых проблем политически мотивированное информационно-психологическое противостояние не ослабевает.

Несмотря на попытки ЕС лавировать между США, Китаем и Россией, сближение с Североатлантическим альянсом и глобальные торговые войны во многом определяют риторику Евросоюза в борьбе с гибридными угрозами. НАТО, на которую Брюссель полагается в сфере безопасности, также использует теорию гибридной войны конъюнктурно, обвиняя в создании военной угрозы «других» в лице России и Китая [Gromyko, 2021: 19]. ЕС, несмотря на стремление к стратегической автономии, в отсутствие собственной армии и в условиях давления со стороны США вынужден участвовать в торговых войнах на стороне Вашингтона, нередко вопреки своим объективным интересам.

Заключение

«Открытая архитектура» теории гибридной войны, широкие возможности трактовки определения гибридных угроз и пополнения их перечня по мере изменения мировых процессов позволяют совершенствовать не только практические меры, но и теоретический подход к проблеме национальной и международной безопасности (учитывать угрозы, исходящие от новых агрессивных политических акторов, злонамеренное использование передовых технологий, последствия недобросовестной конкуренции и т. п.). Однако по мере углубления экономической конкуренции и политических противоречий между государственными акторами подход к противодействию гибридным угрозам гиперполитизируют, используют для оправдания санкционного давления, усиления военных блоков или массированных информационных кампаний против политического оппонента. На пике международных конфликтов противодействие гибридным угрозам может стать обоснованием развертывания как оборонительных, так и наступательных вооружений в мирное время. Дальнейший рост международной напряженности, обусловленный такими явлениями, заставит обвиняе-

---

¹ European Commission, Secretariat-General, 2020. On the European democracy action plan. COM/2020/790 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0790&qid=1632244997810> (дата обращения: 23.09.2021)

мую сторону обороняться. Если эскалация конфликта не остановится, это сделает реальными те гибридные угрозы, которые изначально были мнимыми.

В то же время в мире не ослабевают такие угрозы, как дезинформационные кампании, направленные против международного сотрудничества (в том числе России и ЕС) и против мер защиты граждан в условиях пандемии (в частности, против вакцинации), а также террористическая угроза и т. п. Все это может в решающий момент потребовать усилий всего международного сообщества (которому, увы, сегодня далеко до сплочения в борьбе с мировыми кризисами).

Анализ документов стратегического планирования Европейского союза показывает, что Брюссель формирует и совершенствует системный подход к обеспечению безопасности в условиях гибридизации международных процессов. Этот подход сочетает инициативы в военной, экономической, продовольственной, информационной безопасности и многих других сферах, создавая целостное пространство безопасности интеграционного объединения. Однако экономическое соперничество и политические разногласия коллективного Запада с Россией и Китаем создают политическую конъюнктуру, при которой Пекин и Москву постоянно обвиняют в создании гибридных угроз. В этой ситуации в документах, определяющих подход ЕС к борьбе с гибридными угрозами, необходимость мер безопасности все чаще обясняется злонамеренными действиями государств-оппонентов.

Стоит учитывать, что подход в борьбе с гибридными угрозами в официальных документах ЕС в существующем виде – не только описание стратегии действий институтов Союза, но и всегда – политическая декларация, которая формируется и публикуется под давлением различных групп интересов (зачастую в сугубо тактических целях, например, для оправдания очередного пакета санкций). Такое положение вещей отрицательно сказывается на качестве научных оценок, когда их авторы приспосабливаются к политическому заказу. В политической практике оно ведет к снижению качества международного сотрудничества, в случае ЕС – в первую очередь, с Россией и Китаем, так необходимого на фоне описанных выше угроз. Чрезмерное употребление риторики теории гибридной войны в дискурсе Евросоюза – по сути, акт информационно-психологического противоборства, что ставит под удар безопасность макрорегиона, а для ЕС, стремительно сближающегося с НАТО, – стратегическую автономию.

К сожалению, успешно реализовать подход к противодействию гибридным угрозам (на пользу обществу) в текущих условиях возможно прежде всего при наличии общих для крупнейших стран и объединений Европы угроз (сравнимых по масштабам с претензией террористической организации на формирование собственного государства или угрозой ядерной атаки со стороны преступной организации), осознаваемых политическими элитами как первостепенные. Такие угрозы могут оттеснить политическую конфронтацию на второй план. Разработку стратегического ответа на глобальные вызовы пока тормозит экономическое соперничество.

Чтобы сделать первый шаг к успешной борьбе с гибридными угрозами на глобальном уровне, необходимо совершенствовать существующие подходы с опорой на интересы, прежде всего, граждан. Это не в последнюю очередь задача общественных наук, которые должны преодолеть конъюнктурность, связанную с политическим заказом.

Список литературы

- Белов В.Б. (2021) Коронакризис versus социальное рыночное хозяйство и экономическое пространство Германии. *Современная Европа*. № 4. С. 58–70. DOI: <http://dx.doi.org/10.15211/soveurope420215870>
- Герасимов В.В. (2013) Ценность науки в предвидении, *Военно-промышленный курьер*, № 8 (476), 27 февраля.
- Данилов Д.А. (2021) Россия – ЕС: диалог без диалога. *Научно-аналитический вестник ИЕ РАН*. № 20 (2). С. 7–15, <http://dx.doi.org/10.15211/vestnikieran22021715>
- Панцеров К.А. (2020) Российская гибридная угроза как основополагающий конструкт современной внешнеполитической стратегии Запада. *Война и мир в отечественной и мировой истории*. Санкт-Петербургский государственный университет промышленных технологий и дизайна, Санкт-Петербург, Россия. С. 463–470.
- Потемкина О.Ю. (2020) Новая стратегия Союза Безопасности ЕС. *Аналитические записки ИЕ РАН*. № 32 (№ 215), <http://doi.org/10.15211/analytics322020>

References

- Bazarkina D., Kramar K. (2020) Reputation Management of Russian Companies in the European Union in the Context of Russia and the EU's Strategic Communication, in: Pashentsev E. (ed.) *Strategic Communication in EU-Russia Relations*, Palgrave Macmillan, Cham, Switzerland, https://doi.org/10.1007/978-3-030-27253-1_6
- Belov V.B. (2021) Koronakrizis versus sotsial'noe rynochnoe hozyaystvo i ekonomicheskoe prostranstvo Germanii [The Coronavirus Crisis versus Social and Market Economy of Germany]. *Sovremennaya Evropa*. No 4, pp. 58–70, <http://dx.doi.org/10.15211/soveurope420215870> (in Russian).
- Biscop S. (2021) The EU and China: Sanctions, Signals, and Interests. *Security Policy Brief* No. 145, May. EGMONT – Royal Institute for International Relations, Brussels, Belgium. URL: <https://www.egmontinstitute.be/content/uploads/2021/05/SPB145-revised.pdf?type=pdf> (accessed: 12.10.2021)
- Cusumano E. and Corbe M. (2018) Introduction, in: Cusumano E. and Corbe M. (eds.), *A Civil-Military Response to Hybrid Threats*, Palgrave Macmillan, Cham, Switzerland, https://doi.org/10.1007/978-3-319-60798-6_1
- Danilov D.A. (2021) Rossiya – ES: dialog bez dialoga [Russia – EU: Dialogue without Dialogue]. *Scientific and Analytical Herald of IE RAS*. No 20 (2), pp. 7–15, <http://dx.doi.org/10.15211/vestnikieran22021715> (in Russian).
- Gerasimov V.V. (2013) Tsennost' nauki v predvidenii [The Value of Science in Foresight], *Military-Industrial Courier*, No 8 (476), 27 February. (in Russian).
- Giumelli F., Cusumano E. and Besana M. (2018) From Strategic Communication to Sanctions: The European Union's Approach to Hybrid Threats, in: Cusumano E. and Corbe M. (eds.), *A Civil-Military Response to Hybrid Threats*, Palgrave Macmillan, Cham, Switzerland, https://doi.org/10.1007/978-3-319-60798-6_8
- Gromyko A.I. (2021) Comments on the Brussels Summit Communiqué, 14 June 2021. *Analytical Papers of IE RAN*, vol. III (252), <http://doi.org/10.15211/analytics3220211922>
- Hoffman F. (2009) Hybrid Warfare and Challenges, *Joint Force Quarterly*, vol. 52, pp. 34–39, URL: <https://smallwarsjournal.com/documents/jfqhoffman.pdf> (accessed: 23.09.2021)
- Hoffman F. (2010) 'Hybrid Threats': Neither Omnipotent Nor Unbeatable, *Orbis*, vol. 54. No. 3, pp. 441–455, <https://doi.org/10.1016/j.orbis.2010.04.009>
- Kraft I. (2018) Hybrider Krieg – zu Konjunktur, Dynamik und Funktion eines Konzepts, *Zeitschrift für Außen- und Sicherheitspolitik*, vol. 11, pp. 305–32, <https://doi.org/10.1007/s12399-018-0705-x>
- Krivko M. and Bolgov R. (2021) Special Aspects of Modern Hybrid Warfare on the Internet: Ontological Analysis and Russian Experience, in: Bolgov R., Atnashev V., Gladkiy Y., Leete A., Tsyb A. and Pogodin S. (eds.), *Proceedings of Topical Issues in International Political Geography*, Springer, Cham, Switzerland, https://doi.org/10.1007/978-3-030-58263-0_23
- Lunkin R.N. (2021) Intervention by Roman Lunkin, Deputy Director, Institute of Europe, Russian Academy of Sciences. In: Franco M. (ed.) *How to Reverse in a One Way-Street*. *Egmont Paper* No. 114, September. EGMONT – Royal Institute for International Relations, Brussels, Belgium, pp. 18–20.
- Morillas P. (2019) *Strategy-Making in the EU*, Palgrave Macmillan, Cham, Switzerland, <https://doi.org/10.1007/978-3-319-98627-2>
- Pantserov K.A. (2020) Rossiyskaya gibridnaya ugroza kak osnovopolagajushhiy konstrukt sovremennoy vneshnepoliticheskoy strategii Zapada [Russian hybrid threat as the basis of the current foreign-policy strategy of

the West]. *Voyna i mir v otechestvennoj i mirovoj istorii* [War and peace in the National and world history]. Saint Petersburg State University of Industrial Technologies and Design, Saint Petersburg, Russia, pp. 463–470. (in Russian).

Potemkina O.Yu. (2020) Novaya strategiya Soyuza Bezopasnosti ES [New EU Security Union Strategy], *Analytical Papers of IE RAN*, vol. 32 (215), <http://doi.org/10.15211/analytics322020> (in Russian).

Rinelli S. and Duyvesteyn I. (2018) The Missing Link: Civil-Military Cooperation and Hybrid Wars, in: Cusumano E. and Corbe M. (eds.) *A Civil-Military Response to Hybrid Threats*, Palgrave Macmillan, Cham, Switzerland, https://doi.org/10.1007/978-3-319-60798-6_2

Simons G. (2021) Operational implications and effects of informational and political dimensions of western hybrid warfare, *Bulletin of Moscow Region State University (e-journal)*. No. 3. URL: <https://evestnik-mgou.ru/en/Articles/Doc/1078> (accessed: 23.09.2021)

Evolution of Approaches to Countering Hybrid Threats in the European Union's Strategic Planning

Received 13.10.2021

Author: Bazarkina D., Doctor of Science (Politics), Leading Researcher, Department of European Integration Research, Institute of Europe of the Russian Academy of Sciences. **Address:** 11-3, Mokhovaya Street, Moscow, Russia, 125009. **E-mail:** bazarkina-icspsc@yandex.ru

Abstract. This article aims to identify the main components of the EU approach to countering hybrid threats. To achieve this goal, research questions were posed: 1) How does the theory of hybrid warfare define hybrid threats, what are its strengths and weaknesses? 2) How is the approach to combating hybrid threats regulated in the EU? 3) What changes are taking place in this approach under the influence of trends in recent years, including the crisis caused by the coronavirus pandemic? The author concludes that the “open architecture” of the hybrid war theory, the wide possibilities of interpreting the definition of hybrid threats allow us to improve practical measures and theoretical approaches to security problems. However, as economic competition and political contradictions under geopolitical rivalry deepen, the approach to countering hybrid threats is hyper politicized, being used to justify sanctions pressure, strengthening military blocs or massive psychological campaigns against a political adversary. The EU tries to develop and improve a systemic approach to ensuring security in the context of the growth of hybrid threats. However, this approach is increasingly deformed under the influence of above-mentioned hyperpoliticization. This is especially evident in the EU's attitude towards Russia and China, which are constantly accused of creating hybrid threats. The excessive use of the rhetoric of the hybrid war theory in the EU discourse jeopardizes the security of Europe.

Key words: hybrid threats, hybrid war theory, strategic planning, European Commission, European Parliament, European Union External Action Service.

DOI: <http://dx.doi.org/10.15211/soveurope62021133143>