Современная Европа, 2022, № 2, с. 132–145

ПРОБЛЕМЫ БЕЗОПАСНОСТИ

УДК 32.019.51, 327.8

ПРАКТИКА ПРОТИВОДЕЙСТВИЯ ГИБРИДНЫМ УГРОЗАМ: ОПЫТ ЕВРОПЕЙСКОГО СОЮЗА И ЕГО ГОСУДАРСТВ-ЧЛЕНОВ

© 2022 БАЗАРКИНА Дарья Юрьевна*

Доктор политических наук

Институт Европы РАН. 125009, Россия, Москва, Моховая ул., 11-3.

***E-mail:** bazarkina-icspsc@yandex.ru*

Поступила в редакцию 24.10.2021
После доработки 22.01.2022
Принята к публикации 27.01.2022

Аннотация. В результате роста международной напряженности и распространения гибридных угроз национальные и наднациональные структуры все чаще обращают на них внимание. ЕС адаптируется к новой реальности посредством ведения собственных «гибридных операций». Цель статьи – определить методы и инструменты, посредством которых в ЕС реализуется практика противодействия гибридным угрозам: от борьбы с терроризмом до мер вытеснения экономических конкурентов с европейского рынка. Автор приходит к выводам, что как в институтах ЕС, так и в исследовательском сообществе не создано емкое определение операций борьбы с гибридными угрозами. В пресечении терроризма, киберпреступности, распространения ложных медицинских данных ЕС проявляет системный подход, что позволяет оценить уровень и степень конвергенции угроз, а также возможности противодействия им. Вместе с тем попытки использования экономических, законодательных, политических и информационных инструментов для достижения односторонних экономических, политических и военных преимуществ не снижают градус напряженности в отношениях ЕС с Россией, Китаем и рядом других стран.

Ключевые слова: гибридные операции, гибридные кампании, гибридные угрозы, Европейский союз, Комиссия ЕС, Европейский парламент, Европейская внешнеполитическая служба.

DOI: 10.31857/S0201708322020103

На фоне роста международной напряженности и обвинений государственных акторов в создании гибридных угроз для других стран или интеграционных объединений становится актуальным анализ практики борьбы с гибридными угрозами в национальных и наднациональных структурах. Цель статьи – определить методы и инструменты, посредством которых в ЕС реализуется практика противодействия гибридным угрозам, как с позитивными целями (такими, как борьба с киберпреступностью), так и в рамках вытеснения экономических конкурентов (главным образом, России и Китая) с европейских рынков, а политических оппонентов – из инфосферы. Достижение данной цели требует ответа на исследовательские вопросы: 1) Как определяются операции противодействия гибридным угрозам? 2) Как проводятся в ЕС и его государствах-членах операции по борьбе с гибридными угрозами, актуальными для третьих стран, включая Россию (в частности, с действиями террористических организаций, киберпреступностью и т. п.)? 3) Как подход к противодействию гибридным угрозам используется в ЕС для объяснения мер, принимаемых против экономических конкурентов и политических оппонентов (в особенности в контексте торговых войн США и Китая, напряженности в отношениях США и ЕС с Россией)?

Гибридные угрозы, гибридные кампании и операции противодействия гибридным угрозам: проблемы обозначения

Как в теоретических работах, так и в официальных документах ЕС понятия «гибридные операции» и «гибридные кампании» очень тесно связаны с понятием «гибридные угрозы». Зачастую грань между ними весьма размыта. Так, Ф. Хоффман, труды которого легли в основу теории гибридной войны, в работах разных лет дает практически идентичные определения гибридным войнам [Hoffman, 2007: 29] и угрозам [Hoffman, 2010: 444], указывая на сочетание обычных вооружений, нерегулярной тактики, терроризма и преступного поведения на поле боя. Возможно, это стало одной из причин определенного смешения понятий войны и угрозы как в последующих научных публикациях, так и в стратегических документах, в том числе в ЕС. Тем не менее, если Ф. Хоффман делает акцент, прежде всего, на ведении войны (в том числе и нетрадиционными средствами), то в определениях, данных позже специалистами ЕС и НАТО, понятие гибридных угроз постепенно меняется (к примеру, такие угрозы трактуются как широкое использование противником традиционных и нетрадиционных средств для достижения своих целей[1]).

Европейская внешнеполитическая служба (ЕВС) характеризует гибридные угрозы, прежде всего, как действия, перечисляя их варианты от кибератак до

[1] 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: 15.12.2021)

нарушения поставок энергоносителей[1]. Если понимание угрозы как, например, состояния, способного перерасти в военный конфликт (такая трактовка присутствует в Военной доктрине РФ[2]), все же подразумевает отсутствие этого конфликта и не всегда связано только с субъективным фактором (противником), то угроза как действие всегда подразумевает активную деятельность противника, который в данной ситуации перестает быть предполагаемым, следовательно, и контрмеры будут направлены не столько на урегулирование ситуации, сколько на ограничение возможностей другой стороны. Устойчивое определение операций противодействия гибридным угрозам также до сих пор не разработано, скорее, оно формулируется от противного (борьба с дезинформацией, киберпреступностью, иностранным вмешательством и т. п.). Все это затрудняет теоретический анализ борьбы с гибридными угрозами, в особенности, когда сочетание традиционных и нетрадиционных действий стало свойством самой системы международных отношений [Cusumano and Corbe, 2018: 6]. Однако стоит отметить, что в отношении таких акторов, как преступные и террористические организации, оценка любого действия как угрозы вполне справедлива в силу их изначально антисоциальной сути.

Не менее труден для определения термин «гибридная кампания», еще полностью не оформившийся в научной литературе. В качестве компонентов гибридной кампании выделяются информационные операции (что обосновывает применение контрпропаганды в качестве ответного средства), кибератаки, шпионаж, действия прокси-структур[3] (к примеру, лиц или организаций – проводников пропаганды противника), экономическое и политическое влияние и давление [Mareš, Holzer and Šmíd, 2020: 39–41]. Как и в теоретических работах, так и в подходе ЕС, прослеживаются определенные двойные стандарты: гибридные кампании, действия или операции – всегда то, что реализуется противником, тогда как «противодействие гибридным угрозам» – прерогатива «положительного героя» [это отмечают: Simons, 2021; Fridman, 2018], обозначающего себя как обороняющуюся сторону.

Вместе с тем широкая трактовка гибридных угроз, принятая в ЕС, служит добротным обоснованием инициатив по развитию космической инфраструктуры, здравоохранения, продовольственного обеспечения и т.д. как отраслей обеспечения безопасности общества. Отсюда под мерами противодействия гибридным угрозам понимаются программы защиты критической инфраструктуры, здоровья и т.п. Операции против гибридных угроз в таких сферах подразумевают, к примеру, борьбу с диверсиями в пищевом производстве, с дезинформацией, дискредитирующей научные подходы в медицине, т.е. приносят объективную пользу.

[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: 07.12.2021)

[2] См.: Военная доктрина РФ (утв. Президентом РФ 25 декабря 2014 г. N Пр-2976).

[3] В данном термине можно заметить влияние концепции прокси-войн – конфликтов, в которых третья сторона реализует свои интересы, не принимая открытого участия, но поддерживая одну из противоборствующих сторон (последняя выступает как проводник (“proxy”)) [см.: Mumford, 2013: 40].

Негативную направленность такие операции начинаю приобретать, когда они направлены на выдавливание экономического конкурента, ограничение свободы слова оппонента в информационном пространстве, на расширение военных блоков.

Позитивный опыт противодействия гибридным угрозам в ЕС

Опыт ЕС в борьбе с гибридными угрозами рассмотрен на примерах лишь из нескольких областей (предотвращение терроризма, пресечение его пропаганды, кибербпреступности и дезинформации, связанной с пандемией коронавирусной инфекции). С середины 2020 г. эти угрозы возросли во всем мире, есть прогнозы более широкого использования искусственного интеллекта в преступных целях [Caldwell, Andrews, Tanay and Griffin, 2020]. Пандемию и связанный с ней кризис для распространения своих идей используют экстремисты и террористы. На уровне ЕС за противодействие вышеперечисленным угрозам ответственен ряд агентств, в том числе агентства ЕС по сотрудничеству в правоохранительной сфере (Европол), в области уголовного правосудия (Евроюст) и агентство ЕС по кибербезопасности (ENISA).

Системный подход в противодействии гибридным угрозам реализуется на таких основных направлениях, как модернизация и гармонизация законодательства, перекрытие каналов финансирования акторов гибридных угроз, сотрудничество наднациональных структур ЕС с национальными органами (не только государств-членов, но и третьих стран) в рамках специальных операций. Технические решения в обеспечении безопасности часто предоставляются их разработчиками – частными компаниями. Безусловным достоинством системы борьбы с гибридными угрозами в ЕС можно считать опору на экспертное знание, для получения которого налаживается сотрудничество как можно с большим числом специалистов не только из структур безопасности, но и из гражданской сферы, что позволяет оценить последствия принятых мер для разных групп и слоев общества.

Полезным примером координации оперативной работы правоохранителей ЕС, государств-членов и третьих стран можно считать EMPACT (Европейскую многопрофильную платформу по борьбе с преступностью), объединяющую специалистов из правоохранительных и судебных органов, агентств ЕС, таможенных и налоговых служб, частных компаний. Отчеты Европола используются в рамках EMPACT Комиссией и председателем Совета ЕС для консультирования министров юстиции и внутренних дел, а они принимают приоритеты ЕС в борьбе с преступностью на четыре года за основу национальных оперативных планов действий. Координаторы на уровне ЕС и национальных государств организуют совместные полицейские операции, длящиеся обычно несколько дней или недель[1]. Платформа EMPACT по-

[1] Eurojust, 2021. *EMPACT leaflet*. URL: https://www.eurojust.europa.eu/empact-leaflet (дата обращения: 07.12.2021)

казала свою эффективность, в частности в борьбе с киберпреступностью, среди актуальных примеров – задержание 26 октября 2021 г. двенадцати подозреваемых в кибератаках на критически важную инфраструктуру. В операции приняли участие офицеры из Британии, Германии, Нидерландов, Норвегии, США, Украины, Франции и Швейцарии[1], что показывает высокие возможности координации подобной работы агентствами ЕС, в том числе за его пределами.

Важным подспорьем в борьбе с описываемой группой гибридных угроз остаются экспертные сети, в частности, Информационная сеть по проблеме радикализации (RAN), созданная Комиссией ЕС в 2011 г. и объединяющая 6 тысяч практиков в государствах-членах, работающих с группами, подверженными риску террористической вербовки, а также с активными сочувствующими террористам и экстремистам[2]. Участники сети делятся позитивным опытом, в частности в работе с молодежью или использовании новых ИКТ. Так, в запущенном в 2020 г. в Нидерландах проекте «Игра с полицией» полицейские связываются с молодыми людьми из групп риска в онлайн-играх[3], в настоящее время эту практику осуществляет 21 полицейская группа в стране. Федеральная полиция Бельгии делится практикой опроса детей, возвращенных из зон конфликта на Ближнем Востоке, с использованием специального адаптированного к работе с детьми протокола[4]. Предпринимаются шаги по распространению подобного опыта не только по каналам RAN, но и на площадках ООН.

Сотрудничество правоохранителей и поставщиков цифровых услуг помогает создавать важные практические инструменты борьбы с гибридными угрозами, такие как система электронных доказательств. Проект SIRIUS с 2017 г. реализуется совместно Европолом и Евроюстом в сотрудничестве с Европейской судебной сетью и предлагает руководства, тренинги и инструменты доступа к данным, требующимся в ходе уголовных расследований и хранящимся у поставщиков онлайн-услуг. Эти инструменты доступны правоохранительным и судебным органам через специальную закрытую онлайн-платформу и мобильное приложение[5]. Европол и Евроюст оценивают проект как важный шаг в формализации сотрудничества правоохранителей и частных компаний, однако его работа все еще в большой степени

[1] Europol, 2021. *12 targeted for involvement in ransomware attacks against critical infrastructure*. URL: https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure (дата обращения: 07.12.2021)

[2] European Commission, 2021. *Radicalisation Awareness Network (RAN)*. URL: https://ec.europa.eu/home-affairs/networks/radicalisation-awareness-network-ran_en (дата обращения: 07.12.2021)

[3] European Commission, 2021. *Gaming with the police*. URL: https://ec.europa.eu/home-affairs/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/gaming-police_en (дата обращения: 07.12.2021)

[4] European Commission, 2021. *Interviews of returnee children*. URL: https://ec.europa.eu/home-affairs/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/interviews-returnee-children_en (дата обращения: 07.12.2021)

[5] Europol, 2021. 3rd Annual SIRIUS EU Digital Evidence Situation Report. European Union Agency for Law Enforcement Cooperation, The Hague, Nethderlands, p. 9.

зависит от доброй воли последних. Принятие Закона о цифровых услугах, призванного усилить контроль работы онлайн-платформ со стороны институтов ЕС, ускорит введение обязательной помощи поставщиков цифровых услуг правоохранительным органам.

Борьба с гибридными угрозами означает не только пресечение деятельности преступных акторов, но и проведение информационных кампаний для подготовки общества к защите от растущей угрозы или минимизации информационно-психологического ущерба от действий злоумышленников. В таких кампаниях участвуют представители наднациональных институтов ЕС, национальных правительств, СМИ, бизнеса, институтов гражданского общества. Широко распространено участие агентств ЕС в информационных операциях, среди которых – прекращение по инициативе Европола работы 21 сайта групп, аффилированных с запрещенными в России «Аль-Каидой» и «Исламским государством» в октябре 2021 г.[1] Удаление контента Европолом остается основным методом противодействия пропаганде терроризма в Интернете. Ему на официальном уровне уделяется больше внимания, чем, к примеру, распространению контрнарративов, разрабатываемых, прежде всего, представителями гражданского общества, или перенаправлению пользователей поисковыми системами на сайты, разоблачающие терроризм (метод, реализуемый онлайн-платформами). В пресечении дезинформации, связанной с пандемией, ЕС также опирается на сотрудничество с крупнейшими онлайн-платформами, для которых подписание Кодекса практики по борьбе с дезинформацией сделало эту работу обязательной[2]. На данном направлении используются инструменты мониторинга и ранкинга материалов с помощью искусственного интеллекта, распространение контрнарративов совместными усилиями онлайн-платформ, правительств и СМИ.

Конечно, в агентствах обсуждаются и вопросы иностранного вмешательства в дела ЕС, в настоящее время глубоко политизированные. Европол ссылается на ЕВС, повторяя, что государственные субъекты распространяют дезинформацию, стремясь дестабилизировать управление в Союзе[3], но на официальном сайте ведомства не говорится о конкретной практике борьбы с иностранным вмешательством. Большее внимание проявляет к этой области ENISA, приводящее в своих отчетах данные о спонсируемых государствами (state-sponsored) субъектах кибе-

[1] Europol, 2021. *Germany, the UK and Europol target violent jihadist websites*. URL: https://www.europol.europa.eu/newsroom/news/germany-uk-and-europol-target-violent-jihadist-websites (дата обращения: 07.12.2021)

[2] European Commission, 2021. *Reports on June Actions – Fighting COVID-19 Disinformation Monitoring Programme*. URL: https://digital-strategy.ec.europa.eu/en/library/reports-june-actions-fighting-covid-19-disinformation-monitoring-programme (дата обращения: 07.12.2021)

[3] Europol, 2020. *Catching the virus cybercrime, disinformation and the COVID-19 pandemic*. URL: https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf (дата обращения: 07.12.2021)

ругроз[1], однако специалисты-практики в области безопасности в целом избегают чрезмерно политизированных оценок (в том числе в публикациях, проанализированных выше).

Гиперполитизация противодействия гибридным угрозам

В практике противодействия в иностранному вмешательству в дела ЕС наглядно проявляется чрезмерная политизация, в том числе и в экономических вопросах. Столкновение бизнес-интересов и жесткая конкуренция в принципе присущи капитализму. Однако в настоящее время при обмене обвинениями в гибридных угрозах в экономическое соперничество все сильнее вовлекаются политические элиты. Это в конечном счете сказывается на качестве жизни и информационно-психологической безопасности граждан. В выдавливании китайских и российских компаний с европейского рынка под девизами борьбы с гибридными угрозами можно проследить как экономический интерес местных и американских поставщиков, так и политический интерес «атлантистов» в составе европейской элиты (что снижает не только качество международного сотрудничества ЕС, но и способность европейских союзников США к укреплению реальной стратегической автономии [Данилов, 2021: 19]). Эстония, Латвия и Литва рассматриваются «атлантистами» как первоочередной объект российского гибридного воздействия, что «обусловлено сохраняющейся энергетической зависимостью этих стран от Москвы» [Смирнов, 2020: 15].

Ограничение иностранного влияния предпринимается в ЕС по схеме, напоминающей комплекс мер борьбы с преступными акторами, но имеющей ряд отличий. Так, прямые законодательные запреты деятельности организаций из страны-оппонента (оспариваемые на официальном уровне) могут быть заменены бюрократическими препятствиями (множество этапов рассмотрения контракта, риски наложения вето и т. п.), санкционным давлением (несмотря на то что оно снижает возможности принятия взвешенных решений [Biscop, 2021: 2], выгодных обеим сторонам). Информационно-психологическое воздействие на граждан для дискредитации оппонента осуществляется, как и в борьбе с террористической пропагандой, по всем возможным каналам. Публичные заявления представителей руководства ЕС и государств-членов, политиков, транслирующие сообщение о действиях страны-оппонента как о гибридной угрозе, сопровождаются информационными кампаниями профильных структур (таких, как совместный Центр передового опыта ЕС и НАТО по борьбе с гибридными угрозами) или через профильные издания. Третьи стороны (бизнес-субъекты, частные аналитические центры, представители научного сообщества и т. д.) привлекаются не только для оценки текущего положения или практических решений (к примеру, удаления

[1] ENISA, 2021. *ENISA Threat Landscape 2021*, European Union Agency for Cybersecurity (ENISA), Attiki, Greece, pp. 16–23.

контента, распространяемого оппонентом), но и для публичных политизированных заявлений. Важным информационным рычагом остается установление повестки дня в СМИ.

Показательны в этом отношении информационные кампании с участием правительственных органов и СМИ, проводимые против российского и китайского присутствия на европейском рынке [Seaman, 2021: 7]. Минобороны Швеции заявляет, что «дезинформация и гибридная деятельность, спонсируемая такими государствами, как Китай и Россия, стали частью новой нормы»[1]. Центр «Европейские ценности», участник группы стратегических коммуникаций ЕС на восточном направлении, развернул проект *Kremlin Watch*, где российское руководство обвиняется в попытках давления на страны, экономически зависимые от российских энергоносителей, с целью принудить их поддержать проект «Северный поток-2» [Svárovský et al., 2019: 6].

В странах ЕС государственными структурами распространяются публикации, содержащие обвинения Китая в промышленном шпионаже, а научное сообщество практически прямо именуется его нетрадиционным субъектом (например, в публикации Ведомства по охране Конституции ФРГ[2]). Китайские компании становятся мишенями в атаках на репутацию [Pashentsev, 2020: 15–16]. Все это, конечно, отрицательно сказывается на репутации не только бизнеса, но и самих России и Китая среди европейцев. В 2020 г. крайне негативно относились к России в Швеции, Дании и Нидерландах (по крайней мере, три четверти граждан этих стран)[3]. Рост антикитайских настроений проявился в протестах против создания в центре Европы крупнейшего китайского университета [Шишелина, 2021: 28].

Примером сочетания законодательных и информационных мер можно назвать кампании вытеснения из стран ЕС китайской телекоммуникационной компании *Huawei*. На уровне ЕС в Инструментарии[4] и Отчете об оценке рисков[5] кибербезопасности сетей 5G указывается на возможное вмешательство третьих стран в дела

---

[1] Regeringskansliet, 2021. *"France and Sweden to further develop defence cooperation"*. URL: https://www.government.se/opinion-pieces/2021/09/france-and-sweden-to-further-develop-defence-cooperation/ (дата обращения: 07.12.2021)

[2] Spionageabwehr, 2021. Chinas neue Wege der Spionage. *Single Point of Contact – SPOC*, [online] 1, pp.30-34. URL: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/2021/spoc-wirtschaft-und-wissenschaft-schuetzen.html (дата обращения: 07.12.2021)

[3] Huang C., 2021. *International opinion of Russia and Putin remains negative in 2020*. URL: https://pewrsr.ch/3888Ncl (дата обращения: 07.12.2021)

[4] European Commission, 2020. *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*. URL: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures (дата обращения: 07.12.2021)

[5] European Commission, 2019. *Member States publish a report on EU coordinated risk assessment of 5G networks security*. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 (дата обращения: 07.12.2021)

ЕС, если поставщик 5G имеет прочные связи с правительством страны происхождения или правительство может оказывать давление на поставщика в любой форме. Последний пункт стал предметом спора, так как практически ни одна компания так или иначе не свободна от влияния правительства страны своего базирования. В случае КНР поводом для отказа от сотрудничества в странах ЕС становится Закон о национальной разведке, по которому китайские компании должны сотрудничать с национальной разведывательной службой. В ряде стран ЕС уже запрещено использование китайского оборудования 5G, как в Швеции, где операторы связи до 2025 г. должны исключить его из своей инфраструктуры.

В Бельгии в декабре 2020 г. разразился скандал, в который была вовлечена *Huawei*. Компания проспонсировала статью юриста Э. Вермюльста с критикой протекционистского закона о мерах безопасности при внедрении 5G, вытесняющего китайских производителей с бельгийского рынка. Позже эта статья и несколько других были распространены в *Twitter* с помощью 14 фейковых аккаунтов (как указывает нью-йоркское агентство по расследованиям онлайн-дезинформации *Graphika*, фото профиля в них были сгенерированы с помощью искусственного интеллекта[1]). Представители *Huawei* ретвитнули сообщения с поддельных аккаунтов: по информации *Graphika*, Кевин Лю (руководитель *Huawei* по коммуникациям в Западной Европе), сделал 60 таких ретвитов за три недели, а официальный аккаунт *Huawei Europe* – 47. Агентство признало, что установить, кто стоит за инцидентом, невозможно. Конечно, само то, что менеджеры *Huawei* сделали репосты твитов фейковых профилей, – шаг необдуманный. Однако, несмотря на неопределенность ситуации, несколько бельгийских государственных служащих публично обвинили *Huawei* в атаке на репутацию правительства[2]. Таким образом, информация была введена в уже подготовленную инфосферу, где действия компаний из КНР используются для дискредитации страны.

Как СМИ стран ЕС, так и его правительственные структуры предоставляют площадку политикам, требующим дальнейшего давления на Россию и Беларусь. Об определенных двойных стандартах в борьбе с гибридными угрозами свидетельствует выступление с трибуны Европейского парламента С. Тихановской, которая де-факто открыто призвала к подрыву общественного доверия (одно из гибридных действий, в которых ЕВС обвиняет вероятных противников) к белорусскому президенту, заявив о необходимости для ЕС «использовать “нетрадиционный” подход, обращаясь к белорусскому гражданскому обществу на местах»[3], в частности, инициировав непризнание белорусских властей.

[1] Graphika, 2021. *Fake Cluster Boosts Huawei*. Graphika Reports. URL: https://graphika.com/reports/fake-cluster-boosts-huawei/ (дата обращения: 07.12.2021)

[2] Cimpanu C., 2021. *A network of Twitter bots has attacked the Belgian government's Huawei 5G ban*. URL: https://www.zdnet.com/article/a-network-of-twitter-bots-has-attacked-the-belgian-governments-huawei-5g-ban/ (дата обращения: 07.12.2021)

[3] Agence Europe, 24.11.2021 (Brussels, Belgium).

28 ноября 2021 г. в ходе визита генерального секретаря НАТО Й. Столтенберга в Латвию и Литву председатель Комиссии ЕС У. фон дер Ляйен призвала к более тесному сотрудничеству ЕС и НАТО в борьбе с гибридными атаками[1]. В ходе этой встречи директор совместного Центра передового опыта ЕС и НАТО по борьбе с гибридными угрозами Т. Тииликайнен обвинила Россию, Китай и Иран в использовании нетрадиционных гибридных методов с целью компенсировать недостатки влияния на международном уровне, а правительство Беларуси – в намеренной организации миграционного кризиса[2]. Попытки связать последний с перемещениями российских военных на фоне обвинений в адрес России в планах вторгнуться в Украину – не новость в контексте сообщений об инструментализации миграции с российской стороны (к примеру, в 2015 г. ряд таких публикаций появился в СМИ Финляндии [Alenius, 2021]). Есть основания полагать, что в ЕС в ситуации, когда «интересы в сфере миграционной политики на разных уровнях управления далеко не всегда совпадают, и возникают конфликты» [Потемкина, 2020: 109], возложение вины, прежде всего, на внешних акторов (Беларусь и Россию) используется той частью европейской элиты, которая настроена на дальнейшую конфронтацию.

Заключение

Как в институтах ЕС, так и в исследовательском сообществе, нет емкого определения операций борьбы с гибридными угрозами. В то же время понимание гибридных угроз как *практически любых* (в зависимости от политической конъюнктуры) действий оппонента служит обоснованием применения к последнему *любых* инструментов противодействия.

В борьбе с такими глобальными угрозами, как терроризм, киберпреступность, распространение ложных медицинских данных, ЕС проявляет системный подход, где практика постоянно поддерживается экспертным знанием. Это позволяет не только оценить уровень и степень конвергенции угроз критической инфраструктуре и инфосфере, возможности противодействия, но и постоянно развивать тактики борьбы с ними, привлекая новейшие технические средства и осваивая самые актуальные площадки (свидетельства тому – развитие системы электронных доказательств, совершенствование удаления экстремистского контента, мониторинга и пресечения киберпреступлений, работа с молодежью в зонах ее комфорта, таких, как онлайн-игры, и т. п.). По мере развития подобных инициатив борьба с гибридными угрозами может стать основой стратегической коммуникации ЕС как синхронизации долгосрочной политики и ее коммуникационного сопровождения для внутренней и внешней аудитории.

[1] Agence Europe, 29.11.2021 (Brussels, Belgium).

[2] Hybrid CoE, 2021. *On-going hybrid threats against the EU and NATO*. URL: https://www.hybridcoe.fi/news/on-going-hybrid-threats-against-the-eu-and-nato/ (дата обращения: 07.12.2021)

Вместе с тем в политически острых вопросах, таких, как борьба с иностранным вмешательством, развитая система борьбы с гибридными угрозами, комбинирующая экономические, законодательные и политические инструменты с информационными кампаниями, используется в рамках торговых войн и связанного с ними информационно-психологического противоборства. Это не снижает градус напряженности в отношениях ЕС с Россией, Китаем и рядом других стран, увеличивая количество и силу гибридных угроз, что способно привести к угрозе военной, а также снизить возможности ЕС по достижению стратегической автономии.

СПИСОК ЛИТЕРАТУРЫ

Данилов Д.А. (2021) Глобальные горизонты атлантического альянса: «вакцина» Байдена. *Современная Европа*. № 5. С. 19–31. DOI: http://dx.doi.org/10.15211/soveurope520211931

Потемкина О.Ю. (2020) Многоуровневое управление миграцией в Европейском союзе. *Современная Европа*. № 2. С. 100–110. DOI: http://dx.doi.org/10.15211/soveurope22020100110

Смирнов П.Е. (2020) Эволюция политических приоритетов США в регионе Балтийского моря во втором десятилетии XXI века. *Балтийский регион*. Т. 12. № 3. С. 4–25. DOI: http://dx.doi.org/10.5922/2079-8555-2020-3-1

Шишелина Л.Н. (2021) Триморье: постпандемическое пробуждение. *Научно-аналитический вестник ИЕ РАН*. № 4. С. 24–29. DOI: http://dx.doi.org/10.15211/vestnikieran420212429

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

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

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

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

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

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

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

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

Mumford A. (2013) Proxy Warfare and the Future of Conflict, *The RUSI Journal*, vol. 158, No. 2, pp. 40–46, https://doi.org/10.1080/03071847.2013.787733.

Pashentsev E. (2020) *Coronavirus Pandemics, Huawei 5G Technologies, Artificial Intelligence and Psychological Operations, Geopolitical Report, Vol. 3* (1st ed.), ASRIE Analytica, Rome, Italy.

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

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: 30.11.2021)

Svárovský M., Janda J., Víchová V., Gurney J. and Kröger S. (2019) *Handbook on Countering Russian and Chinese Interference in Europe*, European Values Center for Security Policy, Prague, Czech Republic.

Countermeasures for Hybrid Threats: EU and its Member States Experience

D.Yu. Bazarkina *

Doctor of Science (Politics)

Institute of Europe, Russian Academy of Sciences. Address: 11-3, Mokhovaya street, Moscow, Russia, 125009.

***E-mail:** bazarkina-icspsc@yandex.ru*

Abstract. The article aims to identify the methods and tools used by EU to counter the hybrid threats: from the fight against terrorism to measures aimed at combating economic competitors and political opponents (mainly, to squeeze Russia and China out of European markets). The author concludes that both EU institutions and the research community have not created a comprehensive definition of operations to combat hybrid threats, which is obviously not accidental. A broad understanding of hybrid threats as practically any (depending on the political conjuncture) actions of the opponent serves as a justification for the application of any counteraction tools. In the fight against global threats such as terrorism, cybercrime, and the spread of false medical data, the EU takes a systemic approach, which makes it possible to assess the level and degree of convergence of threats to critical infrastructure and the infosphere, as well as the possibilities of counteraction. At the same time, attempts to use economic, legislative, political and informational tools to achieve unilateral economic, political and military ad-

vantages do not reduce the degree of tension in the EU's relations with Russia, China, and some other countries only increasing the number and strength of hybrid threats. It reduces the EU's ability to achieve strategic autonomy.

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

DOI: 10.31857/S0201708322020103

REFERENCES

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

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

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

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

Danilov D.A. (2021) Global'nye gorizonty atlanticheskogo al'yansa: «vakcina» Bajdena. [Global Horizons of the Atlantic Alliance: the Biden "Vaccine"], *Sovremennaya Evropa*, No 5, pp. 19–31, DOI: http://dx.doi.org/10.15211/soveurope520211931. (In Russian).

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

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

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

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

Mumford A. (2013) Proxy Warfare and the Future of Conflict, *The RUSI Journal*, vol. 158, No. 2, pp. 40–46, https://doi.org/10.1080/03071847.2013.787733.

Pashentsev E. (2020) *Coronavirus Pandemics, Huawei 5G Technologies, Artificial Intelligence and Psychological Operations, Geopolitical Report, Vol. 3* (1st ed.), ASRIE Analytica, Rome, Italy.

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

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

Shishelina L.N. (2021) Trimor'e: postpandemicheskoe probuzhdenie. [The 3 Seas Initiative: Post-Pandemic Awakening], *Nauchno-analiticheskij vestnik IE RAN*, No 22(4), pp. 24–29, http://dx.doi.org/10.15211/vestnikieran420212429. (In Russian).

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: 30.11.2021)

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

Svárovský M., Janda J., Víchová V., Gurney J. and Kröger S. (2019) *Handbook on Countering Russian and Chinese Interference in Europe*, European Values Center for Security Policy, Prague, Czech Republic.