Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Роланд Келемен, *Connections QJ* 22, № 2 (2023): 81-97
https://doi.org/10.11610/Connections.rus.22.2.55

Рецензированная статья

Влияние русско-украинской гибридной войны на политику и правила кибербезопасности Европейского Союза

Роланд Келемен

Университет им. Иштвана Сечени, https://www.uni.sze.hu/

Аннотация: В то время как Россия перешла от гибридной к обычной войне в Украине, НАТО признало киберпространство ещё одной областью, где может понадобиться совместный ответ. Европейский Союз также решил расширить возможности кибербезопасности организации и её стран-участниц, сделав приоритетом устойчивость общества. Признано, что безопасность киберпространства и связанных с ним систем – не только экономическая проблема, она затрагивает всё общество и требует более сложной стратегии и регулирования. ЕС предпринял шаги по смягчению киберрисков, связанных с гибридной войной, повысив сетевую и когнитивную безопасность. Однако наступательные кибероперации всё чаще могут приводить к открытому вооружённому конфликту. В ходе существующих конфликтов некоторые кибероперации могут разрушать доверие общества, усугубляя ситуацию. ЕС и его страны-участницы должны уделять больше внимания динамике эскалации в своём законодательстве и практике. Крайне важно тщательно анализировать киберполитику, ставить конкретные цели и сроки и регулярно обновлять их. Это требует от заинтересованных сторон определения необходимых уровней регулирования и согласования национальных правил, практик и стандартов.

Ключевые слова: гибридная война, когнитивная война, кибербезопасность, Европейский Союз, НАТО, устойчивость.

Вступление

Вооружённое нападение России на Украину в феврале 2022 г. повлияло на концепцию безопасности Европейского Союза. Во многих отношениях его

можно рассматривать как кульминацию предшествующего ему давнего конфликта. Гибридный конфликт, продолжавшийся почти десять лет до полномасштабной войны, также влиял и активно формировал концепцию безопасности ЕС.[1] Меняющиеся взгляды и правила кибербезопасности стали неотъемлемой частью этой трансформации. Высокая степень цифровизации стран-участниц и их обществ сделала их чрезвычайно уязвимыми в киберпространстве.

Важно подчеркнуть, что в контексте данного исследования кибербезопасность — это категория, охватывающая две широкие области: сетевая безопасность и когнитивная безопасность. Сетевая безопасность касается защиты данных в электронных информационных системах и системах управления ими,[2] включая программное обеспечение, оборудование и людей. Когнитивная безопасность означает устойчивость к когнитивному взлому. Инструменты когнитивного взлома включают, среди прочего, фейковые новости, дипфейки и дезинформацию – кибератаки, использующие психологические уязвимости, чтобы в конечном итоге поставить под угрозу логическое и критическое мышление и вызвать диссонанс.[3] Нападения могут быть мотивированы геополитическими устремлениями государства, идеологическими, экстремистскими взглядами и даже экономическими мотивами. Типичным примером является российская гибридная акция, связанная с протестами «жёлтых жилетов» во Франции. Avaaz изучил 100 самых просматриваемых фейковых новостей в Facebook с ноября 2018 по март 2019 гг., связанных с протестом. Это были описания политических акций, направленных против истеблишмента (28 %), жестокости полиции (27 %), нереалистичной и сфабрикованной поддержки движения (19 %), государственной цензуры (14 %), неконтролируемой иммиграции, расизма и ксенофобии (10 %) и другие вопросы (2 %).[4] Россия активно участвовала в распространении фейковых новостей, публикуя их на немецком, испанском, голландском, польском, шведском и итальянском языках. Поразительно, но 100 изученных фейковых сообщений были распространены более чем четырьмя миллионами и просмотрены более чем 105 миллионами человек. Центральный орган кампании дезинформации, RT France, за этот

---

1 James K. Wither, "Hybrid Warfare Revisited: A Battle of 'Buzzwords'," *Connections: The Quarterly Journal* 22, no. 1 (2023): 7-27, https://doi.org/10.11610/Connections.22.1.02.

2 Muha Lajos and Krasznay Csaba, *Az elektronikus információs rendszerek biztonságának menedzselése* (Budapest: Nemzeti Közszolgálati Egyetem, 2019), 11, https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/12932.

3 Kevin Matthe Caramancion, Li Yueqi, Elisabeth Dubois, and Ellie Seoe Jung, "The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats," *Data* 7, no. 4 (2022): 49, https://doi.org/10.3390/data7040049.

4 "Yellow Vests Flooded by Fake News: Over 100M Views of Disinformation on Facebook," *Avaaz Report*, March 15, 2019, accessed October 12, 2023, 5-6, www.politico.eu/wp-content/uploads/2019/03/AVAAZ_YellowVests_100miofake.pdf.pdf.pdf.

период набрал более 30 миллионов просмотров.[5] Уже одни эти данные говорят об эффективности такой гибридной кампании дезинформации. Если добавить к этому скорость распространения сообщений, масштаб проблемы станет ещё более очевидным. Например, в одном фейковом посте были изображены мирные жители с окровавленными головами, с утверждением, что они стали жертвами жестокости полиции. Этим постом, опубликованным 20 ноября 2018 г., поделились 136 000 человек, а просмотрели его свыше 3,5 млн. Позже выяснилось, что фотографии были сделаны в разных странах в разное время, а целью компиляции было изобразить жестокость полиции, радикализировать протестующих и пробудить солидарность общества во Франции и других странах.[6] Таким образом, когнитивная безопасность стала неотъемлемой частью кибербезопасности, во многом из-за гибридной деятельности России и развития соцсетей. Основное различие между сетевой безопасностью и когнитивной безопасностью заключается в их целях: в то время как классические кибератаки нацелены на ИТ-системы, когнитивные атаки направлены на подкомплексы членов общества. Эти две области не всегда резко отличаются. Они часто дополняют друг друга, повышая общую эффективность.

Инструментарий гибридности в киберпространстве позволил атаковать не только (социальные) сети государств, вовлеченных в гибридный конфликт, но и сети геополитических соперников. В случае этих гибридных угроз вероятность открытой военной конфронтации относительно низка. Вместо этого использование гибридных средств направлено на отстаивание интересов в геополитическом противостоянии и ослабление враждебных групп.[7] Российское государство ведёт очень современную гибридную войну. По словам Махмута Гареева, Россия стремится достичь политических целей в информационной войне, не прибегая к военной силе. Это создаёт так называемый контролируемый хаос в государстве, против которого она направлена. Герасимов добавил, что её конечной целью является подрыв способности к самоорганизации атакованного государства.[8]

---

5 Jarmo Makela, “Countering Disinformation: News Media and Legal Resilience,” Hybrid CoE Paper 1, Workshop organized by the Hybrid CoE and the Media Pool, part of the Finnish Emergency Supply Organization, April 24-25, 2019 (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, November 2019), 10-13, https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf.

6 Avaaz Report “Yellow Vests Flooded by Fake News,” 21-22.

7 Ádám Farkas, *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon* (Budapest: Magyar Katonai Jogi és Hadijogi Társaság, 2022), 35.

8 Katri Pynnöniemi, “The Concept of Hybrid War in Russia: A National Security Threat and Means of Strategic Coercion,” *Hybrid CoE Strategic Analysis* 27, Hybrid CoE, May 18, 2021, 4-5, https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-27-the-concept-of-hybrid-war-in-russia-a-national-security-threat-and-means-of-strategic-coercion/.

В результате, хотя страны-участницы ЕС не были напрямую вовлечены в российско-украинский гибридный конфликт и войну, их сети были атакованы, что потребовало серьёзных шагов по усилению их кибербезопасности. В этой статье мы рассмотрим меры, которые ЕС пришлось принять в области кибербезопасности (сетевой и когнитивной) из-за событий между Россией и Украиной. Исследование охватывает два периода: 10 лет до начала крупномасштабной российской агрессии, характеризующиеся преимущественно гибридным конфликтом, и период непосредственно перед и во время войны.

Реакция ЕС на вызовы периода гибридного конфликта

В начале 2010-х гг. Евросоюз признал необходимость вмешательства в сферу кибербезопасности. Эта проблема по своей сути является международной и затрагивает всё сообщество. Без сотрудничества, поддержки, руководства, координации и содействия совместным действиям страны-участницы не смогут эффективно решать долгосрочные проблемы и вызовы кибербезопасности.[9]

Комиссия и Верховный представитель ЕС по иностранным делам и политике безопасности совместно разработали стратегию кибербезопасности ЕС. Стратегия представляет почти утопическое видение киберпространства,[10] напоминающее начало 2000-х годов, время появления Web 2.0. В этом видении киберпространство способствует политической и социальной интеграции, разрушает барьеры между странами, сообществами и гражданами;[11] там соблюдаются основные права и свободы. Один из ключевых элементов международной киберполитики ЕС – сохранить киберпространство как место, где гарантированы основные права и свободы.[12] Эта стратегия предполагала, что киберпространство может выполнить свою миссию только в том случае, если полностью соблюдаются традиционные нормы ЕС.[13] Она также обозначила пять стратегических приоритетов реализации этих принципов:

1. Обеспечение устойчивости к кибератакам;
2. Резкое снижение киберпреступности;

---

9 Helena Carrapico and Andre Barrinha, “European Union Cyber Security as an Emerging Research and Policy Field,” *European Politics and Society* 19, no. 3 (2018): 299-303, https://doi.org/10.1080/23745118.2018.1430712.

10 Gergely Gosztonyi, “Aspects of the History of Internet Regulation from Web 1.0 to Web 2.0,” *Journal on European History of Law* 13, no. 1 (2022): 168-173.

11 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace” (Brussels: European Commission, February 7, 2013), Join(2013) 1 final, 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001.

12 “Cybersecurity Strategy of the European Union” (2013), 17.

13 “Cybersecurity Strategy of the European Union” (2013), 4.

3. Разработка политики и средств киберзащиты для Общей политики безопасности и обороны (ОПБО);[14]
4. Развитие промышленных и технологических ресурсов кибербезопасности;
5. Выработка последовательной международной политики Евросоюза в киберпространстве и продвижение основных ценностей ЕС.[15]

Стратегия кибербезопасности в общих чертах описывает мотивы кибератак, включая преступные действия (отдельных лиц или групп), терроризм, политически мотивированные атаки и кибератаки, организованные государством. Евросоюз разработал правовые нормы для более решительной и эффективной борьбы с киберпреступностью и кибертерроризмом. Однако в том, что касается деятельности в киберпространстве, которая затрагивает международное право, например кибератаки и их атрибуция, киберсуверенитет, вооружённые нападения и самооборона государства, в Стратегии говорится, что «Союз не ожидает создания международно-правовых инструментов по вопросам киберпространства».[16] Последствия этой ошибочной позиции проявились к концу десятилетия, особенно во время русско-украинского противостояния и войны, разразившейся в феврале 2022 года. Конфликт показал необходимость жёстких международно-правовых инструментов в киберпространстве, учитывая широкое использование инструментов гибридной войны. В ответ ЕС запустил свой набор инструментов кибердипломатии, чтобы хотя бы частично восполнить этот пробел.

Стратегия 2013 года не способна адекватно отразить уникальные характеристики киберпространства, которое существенно отличается от традиционного физического пространства. В итоге она не даёт чёткой основы для применения основных ценностей ЕС конкретно к киберпространству и не затрагивает отдельных характеристик киберпространства, проявляющихся только там.[17] Более того, из-за международного характера киберпространства и различий в нормативно-правовой базе стран-участниц ЕС, в ЕС сочли

---

[14] László Knapp, "A terrorizmus elleni küzdelem az Európai Unió jogában: A terrortámadásra adandó válasz a szolidaritási és a kollektív védelmi klauzula tükrében," *A terrorizmus elleni küzdelem aktuális kérdései a XXI. Században,* ed. Róbert Bartkó (Budapest: Gondolat Kiadó, 2019), 119-136, https://dfk-online.sze.hu/a-terrorizmus-elleni-kuzdelem-aktualis-kerdesei-a-xxi-szazadban.

[15] "Cybersecurity Strategy of the European Union (2013)," 5.

[16] "Cybersecurity Strategy of the European Union (2013)," 18.

[17] К таким характеристикам относятся изменение понятий о геометрическом пространстве, преодоление традиционных представлений о географическом расстоянии, разграничение внутреннего и внешнего киберпространства, а также использование теорий расслоения (которые необходимы для идентификации объектов регулирования). Кроме того, это предполагает преодоление линейной или гипердифференцированной природы норм и обучения (супер-гипер-дифференциация), метаморфозу социальных отношений (например, увеличение способности к синдикации и гибкость социальных сетей) и релятивизацию понятия времени. Также происходят изменения в предмете фундаментальных прав

невозможным развивать централизованный европейский надзор. Поэтому инициативу в области кибербезопасности проявляли преимущественно отдельные страны-участницы и частный сектор.[18] Подход Евросоюза критиковали как контрпродуктивный, в частности потому, что его основной целью в тот период была определена гармонизация норм. Эта цель требует либо создания центрального института ЕС с более широкими полномочиями, чем у ENISA,[19] либо расширения возможностей ENISA по координации деятельности национальных правительств и по разработке и внедрению единого протокола защиты. Первоначальная позиция ЕС оказалась ошибочной, но предпринимаются усилия изменить её. Переоценке способствовали такие факторы, как растущее влияние соцсетей, их коммерциализация и последствия для безопасности и общества,[20] а также продвижение гибридных сценариев из России и Китая в последние годы. Тем не менее, признание важности защиты киберпространства для защиты традиционных пространств стало важным шагом вперёд.

Незаконная аннексия Крыма и поддержка Россией сепаратистов на Донбассе в 2014-2015 гг., а также их последствия в киберпространстве вынудили ЕС принять меры. В 2015 г. Совет Европейского Союза опубликовал свои Выводы о кибердипломатии, где кибербезопасность, права человека, международное право и верховенство права в киберпространстве отмечены как постоянные проблемы общей внешней политики и политики безопасности. Совет подчеркнул, что эти проблемы можно решить только посредством всеобъемлющей, комплексной и последовательной международной политики в киберпространстве. Он также отметил важность продвижения и защиты единого, открытого, свободного и безопасного киберпространства, чего можно достичь только путём полного уважения основных ценностей ЕС: демократии, прав человека и верховенства права. С этой целью в документе указано, что необходим последовательный и всеобъемлющий подход ЕС к кибердипломатии, и он был одобрен два года спустя.[21] Поставленные цели, такие, как сохранение фундаментальных ценностей, уважение свобод, гендерное равенство, конкуренция и благополучие, также высветили существенные различия в понимании кибербезопасности между

(например, данные, активы в играх), их характеристиках (при этом социальные сети становятся наиболее важным пространством для свободы самовыражения) и их ограничениях (например, частное курирование).

18 “Cybersecurity Strategy of the European Union (2013),” 19.

19 European Union Agency for Cybersecurity.

20 Enikő Kovács-Szépvölgyi, “A digitális gyermekvédelem egyes aspektusai,” *Széchenyi István Egyetem Új Nemzeti Kiválóság Program Tanulmánykötet 2021/2022* (Győr: Széchenyi István Egyetem, 2022), 227-236, https://tud.sze.hu/images/%C3%9ANKP/2021-2022/UNKP_2022_0725_Tanulma%CC%81nyko%CC%88tet%20beli%CC%81v.pdf.

21 Council of the European Union, “Council Conclusions on Cyber Diplomacy,” 6122/15, Brussels, February 11, 2015 (OR. en), https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

западными и восточными странами, которые уже становились очевидными как геополитические разломы.

После действий России против Украины Европейский Союз также признал важность решения проблемы гибридности, включая дезинформацию. В ответ в 2015 г. была создана оперативная группа East StratCom для усиления возможностей ЕС предвидеть, обнаруживать и реагировать на дезинформацию со стороны внешних сил.

В сообщении Комиссии от 2016 года, в том числе о киберпространстве, сказано, что несмотря на позитивные изменения, ЕС остается уязвимым для инцидентов в области кибербезопасности. Отмечено, что операции в киберпространстве, зачастую являющиеся инструментами гибридных атак, представляют серьёзную опасность.[22] Эти атаки, совершаемые теми, от кого исходит гибридная угроза, «могут даже привести к дестабилизации стран или политических институтов».[23]

Не случайно в ЕС почувствовали необходимость адаптировать и обновить Стратегию 2013 года, что вылилось в её доработку в 2017 г. Во введении к Стратегии говорится, что с годами угрозы росли в геометрической прогрессии, а кибербезопасность имеет основополагающее значение для безопасности повседневной жизни. Кибератаки могут совершать государственные и негосударственные субъекты, что стирает грань между традиционными субъектами и субъектами безопасности в киберпространстве. Стратегия подчёркивает, что некоторые государства навязывают свои геополитические интересы посредством операций в киберпространстве, и предупреждает, что если ЕС не сможет существенно повысить свою кибербезопасность, с развитием цифровизации риск будет расти. В стратегии утверждается, что устойчивость ЕС к кибератакам является реальной целью, если будет решён ряд задач: укрепление ENISA; полная реализация Директивы сетевой и информационной безопасности (NIS);[24] быстрое реагирование на чрезвычайные ситуации как залог устойчивости; активизация НИОКР; созда-

---

[22] European Commission, 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/2016/018 final/3, point 4.4 Cybersecurity, Brussels, April 6, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018.

[23] "Opinion of the European Economic and Social Committee on the 'Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry' (COM(2016) 410 final)," Document 52016AE4559, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016AE4559.

[24] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union," https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

ние базы кибернавыков, в т.ч. путём улучшения образования; и продвижение кибергигиены и осведомленности.[25]

В 2017 году, через два года после провозглашения единой кибердипломатии ЕС, Совет Европейского Союза ввёл в действие Инструментарий кибердипломатии – инструмент общего реагирования ЕС на злонамеренную кибердеятельность. Этот набор инструментов предназначен для предотвращения конфликтов, смягчения угроз кибербезопасности и стабилизации международных отношений. Дипломатический ответ ЕС должен быть пропорционален объёму, масштабу, продолжительности, интенсивности, сложности, изощрённости и эффекту любой киберактивности. Набор инструментов был дополнительно детализирован в 2019 г. Регламентом и Решением Совета. Эти правила применяются в случае кибератаки со значительным внешним воздействием или попытки кибератаки против ЕС или одной из его стран-участниц. Атаками считаются незаконные действия, направленные на доступ к информационной системе, вмешательство в неё или её мониторинг. Злонамеренными считаются, в частности, атаки на критическую инфраструктуру, системы, обеспечивающие важную социальную и экономическую деятельность, системы поддержания важных государственных функций, и правительственные группы реагирования. Для определения значительного воздействия учитывают такие факторы, как объём и масштаб нарушений, количество атакованных физических или юридических лиц, организаций и стран-участниц ЕС, причинённый экономический ущерб, а также объём и масштаб затронутых данных. Это позволяет ЕС препятствовать проникновению или транзиту лиц, совершивших такие атаки, на территорию Союза, а также замораживать их средства и активы.[26] Эти положения недвусмысленно свидетельствуют о намерении Союза наказать внешних злоумышленников за атаки второй половины 2010-х гг. ЕС действовал решительно, создав правовой режим, использующий набор инструментов кибердипломатии и санкции в рамках общей внешней политики и политики безопасности. В июле 2020 г. Совет Европейского Союза ввёл санкции против российских, китайских и северокорейских хакеров, причастных к таким кибератакам, как Wannacry и NotPetya. Кроме того, в октябре 2020 г. были введены санкции против российских хакеров, участвовавших в кибератаках

[25] European Commission, “Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU (JOIN/2017/0450 final),” Document 52017JC0450, Brussels, September 13, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN.

[26] “Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States,” https://eur-lex.europa.eu/eli/reg/2019/796/oj; “Council Decision (CFSP) 2019/797 of 17 May 2019 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States,” https://eur-lex.europa.eu/eli/dec/2019/797/oj.

на парламент Германии в 2015 г. Санкциям подверглись восемь частных лиц и четыре организации.[27]

В 2018 г. ЕС утвердил План действий по борьбе с дезинформацией, распределив полномочия между национальными органами и институтами ЕС. Скоординированное реагирование основано на четырёх принципах:

(1) Усиление возможностей институтов ЕС;

(2) Скоординированная реакция на дезинформацию;

(3) Мобилизация частного сектора;

(4) Повышение устойчивости общества.

Планом предусмотрена поддержка органов ЕС, способных внести свой вклад в эти усилия, создание системы оповещения, способной в реальном масштабе времени сообщать о дезинформации, а также назначение ответственных в странах-участницах. Мобилизуя частный сектор, документ отметил роль и ответственность платформ, указав на их предыдущие упущения в эффективном решении проблемы.[28]

Согласно Плану действий, в 2019 г. была создана Система быстрого оповещения для облегчения обмена информацией и координации противодействия дезинформации национальных учреждений и институтов ЕС. Система включает сеть из 27 ответственных в отдельных странах для координации усилий и обмена передовым опытом. Однако разделение компетенции между различными организациями может усложнить решение проблем, и национальный инструментарий остаётся основным ресурсом для решения этих вопросов.[29] Пандемия COVID-19 выдвинула на первый план проблему дезинформации, порождающую так называемую инфодемию. Она показала, что ЕС необходимо различать разные формы ложного или вводящего в заблуждение контента, например, незаконный – и вредный, но законный контент. В последнем случае дезинформация означает ложную или вводящую в заблуждение информацию, опубликованную с намерением обмануть, нанести вред общественным интересам или экономический ущерб. Основу противодействия дезинформации составляют предыдущий План действий, Кодекс правил и практика Группы быстрого реагирова-

[27] Miftahul Khausar and Abdul Rivai Ras, “Establishment of the Cyber Diplomacy Toolbox (CDT) as a Joint Diplomatic Response to the European Union against the Threat of Cyber Attack Activity,” *Politicon – Jurnal Ilmu Politik* 5, no. 1 (2023): 29-58, https://journal.uinsgd.ac.id/index.php/politicon/article/view/14833.

[28] European Commission, “Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Action Plan against Disinformation,” JOIN(2018) 36 final, Brussels, December 5, 2018, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018JC0036.

[29] Makela, “Countering Disinformation: News Media and Legal Resilience,” 15.

ния.[30] Однако главные задачи борьбы с дезинформацией на платформах ложатся на провайдеров платформ.

В декабре 2020 г. Европейская комиссия представила План действий по развитию демократии в Европе, четвёртый пункт которого посвящён борьбе с дезинформацией. В этой части плана подчёркнута необходимость более тесного сотрудничества с частным сектором, гражданским обществом, научными кругами и международными партнёрами ЕС для лучшего понимания гибридных угроз и противодействия им. Документ критикует платформы за непрозрачность их алгоритмов и подачу новостей – проблемы, выявленные в ходе оценки Кодекса правил. Комиссия считает, что для эффективного противодействия дезинформации нужны более строгие и чёткие обязательства провайдеров платформ и подход, основанный на механизме надлежащего надзора.[31] Согласно Плану действий, Комиссия в 2020 г. предложила Закон о цифровых услугах (Digital Services Act, DSA), который был принят осенью 2022 г. Цель DSA – создание безопасной, предсказуемой и заслуживающей доверия онлайн-среды, где уважаются права, закреплённые в Хартии основных прав.

Меры ЕС в области кибербезопасности на фоне русско-украинской войны

В конце 2020 г. Евросоюз чётко продемонстрировал намерение усилить интеграцию в сфере кибербезопасности. Новая стратегия – откровенная и убедительная демонстрация того, что Евросоюз в целом понимает проблемы киберпространства. Согласно Стратегии, «кибербезопасность является неотъемлемой частью безопасности европейцев ... Транспорт, энергетика, здравоохранение, телекоммуникации, финансы, безопасность, космос, оборона и демократические процессы крайне зависят от всё более взаимосвязанных сетей и информационных систем».[32] Пандемия COVID-19 усилила

[30] European Commission, “Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Tackling COVID-19 disinformation – Getting the Facts Right,” JOIN(2020) 8 final, Brussels, June 10, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0008.

[31] European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – On the European Democracy Action Plan,” COM(2020) 790 final, Brussels, December 3, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN.

[32] European Commission, “Joint Communication to the European Parliament and the Council – The EU’s Cybersecurity Strategy for the Digital Decade,” JOIN/2020/18 final, Brussels, December 16, 2020, 1, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018.

эти тенденции, ускорив цифровизацию.[33] Сбои в цепочке поставок серверных технологий создают серьёзную проблему и приводят к геополитической напряжённости. Растущее число вредоносных атак на критическую инфраструктуру в последние годы также вызывает обеспокоенность. Они препятствуют использованию онлайн-услуг и в конечном счёте наносят экономический ущерб. Решение этих проблем затягивается, а раскрываемость преступлений остаётся низкой. В Стратегии далее отмечено, что киберпреступность растёт, а киберготовность и осведомлённость о кибербезопасности предприятий и частных лиц остаётся на низком уровне. Кроме того, сотрудникам не хватает навыков кибербезопасности. За этот недостаток несут ответственность не только страны-участницы, но и ЕС в целом. Мало программ, помогающих людям наверстать упущенное. Тем не менее большинство существующих инициатив используют шаблонный подход, который не может эффективно удовлетворить потребность в улучшении навыков кибербезопасности.[34]

За последнее 10 лет ЕС прошёл большой путь. Первоначально основное внимание уделялось экономическим последствиям киберугроз. В настоящее время существует чёткое понимание, что кибербезопасность – это проблема всего общества, требующая всестороннего внимания. Менее заметно понимание того, что кибербезопасность – не только техническая проблема; она требует междисциплинарного подхода, сочетающего образование, исследования и нормативное регулирование.

Опираясь на достижения предыдущих стратегий, ЕС считает необходимым использование трёх основных инструментов – регулирования, инвестиций и политики – для действий в трёх областях:

1. устойчивость, технологический суверенитет и лидерство;
2. наращивание оперативных возможностей для предотвращения, сдерживания и реагирования;
3. продвижение глобального, открытого киберпространства.[35]

Их реализация будет связана с крупными цифровыми инвестициями в течение следующих семи лет, что позволит объединить целый ряд стимулов, обязательств и ориентиров с упором на искусственный интеллект, шифрование и квантовые вычисления. Одним из главных инструментов тут станет Европейский фонд обороны (EDF). Эти три основные области можно разделить на подобласти. Устойчивость, технологический суверенитет и лидерство опираются на:

а) устойчивую инфраструктуру и критически важные услуги;

---

[33] Ferencz Jácint, “Blokchain-rendszerű megoldások a munkaviszonyban,” *Erdélyi Jogélet* 1, no. 4 (2020): 21-28, https://doi.org/10.47745/ERJOG.2020.04.02.

[34] European Commission, “Joint Communication to the European Parliament and the Council – The EU’s Cybersecurity Strategy for the Digital Decade,” 1-4.

[35] European Commission, “Joint Communication to the European Parliament and the Council – The EU’s Cybersecurity Strategy for the Digital Decade,” 5.

b) создание европейского киберщита;
c) сверхзащищённую инфраструктуру связи;
d) обеспечение безопасности сетей мобильной широкополосной связи следующего поколения;
e) безопасную среду после Интернета вещей (IoT);
f) повышение глобальной кибербезопасности;
g) более активное присутствие в цепочке поставок технологий;
h) кибернавыки рабочей силы в ЕС.[36]

Некоторые из этих целей представляются достижимыми на уровне ЕС – такие, как изменение нормативной базы (например, Директива NIS2 [37] и Регламент DORA,[38] Цифровая повестка дня), повышение устойчивости общества и разработка индивидуальных программ. Однако некоторые формулировки, такие, как «сверхзащищённая система», «европейский киберщит» и «повышение безопасности глобального Интернета», звучат как пропаганда, находятся вне влияния сообщества и поэтому не представляются реалистичными целями.

Наращивание оперативных возможностей для предотвращения, сдерживания и реагирования предусматривает:

a) общее подразделение кибербезопасности;
b) борьбу с киберпреступностью;
c) активное использование инструментов кибердипломатии ЕС;
d) развитие возможностей киберзащиты.

Создание совместного подразделения кибербезопасности – новый шаг, раньше в ЕС не хотели создавать такой орган. В документе подчёркивается, что это значительно усилит реакцию Европы на кризисы кибербезопасности. Совместное подразделение кибербезопасности будет выполнять три главные задачи: повышение готовности сообществ кибербезопасности, повышение осведомленности о ситуации за счёт лучшего обмена информацией, и совершенствование совместного реагирования.[39] В выводах Совета

[36] European Commission, "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade," 6-14.

[37] "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)," PE/32/2022/REV/2, https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[38] "Digital Operational Resilience Act (DORA) – Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

[39] European Commission, "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade," 14-22.

ЕС от октября 2021 г. подтверждено, что страны-участницы согласны создать такой институт, хотя присоединение к нему будет добровольным.

Продвигая глобальное и открытое киберпространство, ЕС стремится взять на себя ведущую роль в разработке и совершенствовании стандартов, правил и принципов киберпространства. Однако эти амбиции выглядят утопическими, учитывая нынешнюю геополитическую роль ЕС, поскольку США и Китай обладают намного большими ресурсами в этой области. Кроме того, ЕС стремится двигаться к созданию добровольных, необязательных норм ответственного поведения государств под эгидой ООН. Однако этот план вряд ли приведёт к существенным изменениям, поскольку отсутствие реальных санкций означает, что ситуативная власть и политические интересы, скорее всего, будут перевешивать кодекс поведения. Другие вопросы, такие как сотрудничество, укрепление партнёрства и повышение устойчивости в мировом масштабе, повторяются и не дают ничего нового.[40]

Новая стратегия кибербезопасности – серьёзный шаг в сторону более реалистичного подхода, особенно в плане признания необходимости создания общей структуры. Однако некоторые цели остаются утопическими, возможно, из-за неправильной оценки ЕС своего геополитического положения и глобальных реалий. Тем не менее новый регламент может повысить эффективность оперативной кибербезопасности сообщества.

Начало войны активизировало сотрудничество между НАТО и ЕС, что дало заметные результаты в области кибербезопасности, часто – в военных терминах. Так, центральной темой саммита НАТО 2022 г. в Мадриде стала русско-украинская война, поддержка Украины и поиск окончания войны. В итоговом документе подчёркнуто укрепление стратегического партнёрства при уважении целостности обеих организаций, подкрёпленное их совместной поддержкой Украины. Киберпространство осталось важной темой. В коммюнике саммита сказано, что кибернетические, космические, гибридные и другие асимметричные угрозы, а также злонамеренное использование новых разрушительных технологий необходимо решать совместно.[41] Обе организации намерены и дальше поддерживать Украину в борьбе с Россией, включая предоставление нелетального оборонительного оборудования для усиления киберзащиты и устойчивости Украины.[42] На фоне русско-украинской войны приоритетом стала энергетическая безопасность. Цель – ускорить адаптацию Альянса и повысить устойчивость к кибернетическим и гибридным угрозам за счёт комплексного применения политических и военных инструментов. НАТО существенно усиливает свою киберза-

[40] European Commission, “Joint Communication to the European Parliament and the Council – The EU’s Cybersecurity Strategy for the Digital Decade,” 22-28.

[41] NATO, “Madrid Summit Declaration,” issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid, June 29, 2022, articles 6, 15, https://www.nato.int/cps/en/natohq/official_texts_196951.htm.

[42] “Madrid Summit Declaration,” point 8.

щиту, расширяя военно-гражданское сотрудничество и партнёрство с промышленностью.[43] Эти вопросы нашли отражение, например, в Регламенте NIS2, где значительная часть задействованной инфраструктуры предназначена для обеспечения кибербезопасности цепочек поставки.

На саммите в Мадриде Альянс объявил о новой Стратегической концепции, в которой изложены пять ключевых целей и принципов.

1. НАТО полна решимости защищать свободу и безопасность союзников от угроз со всех направлений.
2. Альянс необходим для безопасности региона, основанной на ценностях свободы личности, прав человека, демократии и верховенства права. Эти принципы соответствуют целям и принципам Европейского Союза.
3. НАТО является уникальной и незаменимой платформой для координации и действий в области индивидуальной и коллективной безопасности. Её приверженность безопасности, солидарности и взаимной обороне неделима.
4. Эта решимость опирается на возможности сдерживания и обороны Североатлантического союза.
5. У НАТО три основных функции: сдерживание и оборона, предотвращение и урегулирование кризисов, и сотрудничество ради безопасности.

НАТО повысит индивидуальную и коллективную устойчивость и увеличит своё технологическое преимущество, столь важное для решения основных задач Североатлантического союза.[44] Во всех документах после 2018 г. отмечаются общие трансатлантические ценности, составляющие основу альянса, и важность сотрудничества с Европейским Союзом. Эти документы описывают среду безопасности и подчёркивают, что враждебные авторитарные государства используют взаимосвязь, открытость и высокую степень цифровизации, характерную для стран НАТО, для вредоносной деятельности в киберпространстве, включая дезинформацию. Россия, считающаяся главной и прямой угрозой в Евроатлантике, использует против Альянса традиционные, кибернетические и гибридные средства. Киберпространство признано областью особой важности, так как злоумышленники стремятся разрушить критическую инфраструктуру, нарушить работу государственных служб, получить разведданные, украсть интеллектуальную собственность и помешать военной деятельности НАТО.[45]

Согласно духу Итогового документа, Европейский Союз предпринял важные шаги по укреплению кибербезопасности Украины после начала войны.

---

[43] “Madrid Summit Declaration,” art. 10.

[44] “NATO 2022 Strategic Concept,” adopted by Heads of State and Government at the NATO Summit in Madrid, June 29, 2022, 3, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

[45] “NATO 2022 Strategic Concept,” 3-4.

С марта 2022 по февраль 2023 гг. ЕС выделил на эти цели почти 11 млн. евро. Основная цель заключалась в удовлетворении потребностей украинских властей в кибербезопасности и безопасности данных, уделяя особое внимание замене уничтоженного оборудования и обеспечению непрерывной работы государственных служб во время войны. Эстонская Академия электронного управления возглавила реализацию проекта, используя свой опыт в области цифрового управления и кибербезопасности для поддержки Украины в это трудное время.[46]

ЕС и Украина поддерживают диалог в области кибербезопасности с начала войны, уделяя особое внимание повышению устойчивости. По оценке Европейской службы внешних связей, «благодаря тесному сотрудничеству с ЕС и другими международными партнёрами в области кибербезопасности и киберзащиты Украина продемонстрировала впечатляющие возможности по отражению кибератак и защите критической инфраструктуры».[47]

В итоговом документе Вильнюсского саммита НАТО 2023 г. подтверждено, что Альянс и его члены связывают общие ценности прав человека, демократии и верховенства права. Подчёркнута необходимость укрепления такого единства перед лицом войны на континенте и усиления безопасности НАТО со всех направлений. Укрепление национальной и коллективной устойчивости является важной частью этой стратегии, наряду с сотрудничеством с Европейским Союзом, как уникальным и незаменимым партнёром НАТО для процветания и безопасности евроатлантического региона. Это необходимо и потому, что Россия и Китай ещё больше активизировали свою деятельность, включая гибридные и кибератаки против Альянса, вмешательство в демократические процессы и другие подрывные действия. Война России с Украиной чётко показала, насколько киберпространство является частью современного вооружённого конфликта, причём такие инциденты могут быть приравнены к вооружённому нападению согласно статье 51 Устава ООН, что позволяет задействовать статью 5 Вашингтонского договора, *casus foederis*. Поэтому НАТО увеличит вклад киберзащиты в потенциал сдерживания путём дальнейшего развития трёх уровней киберзащиты — политического, военного и технического. Этот подход обеспечит военно-гражданское сотрудничество в условиях мира, кризиса и конфликта, включая, при необходимости, сотрудничество с частным сектором, что повысит общую ситуационную осведомленность. Однако для достижения успеха необходим активный вклад стран НАТО, не входящих в ЕС, в усилия стран-участниц ЕС. Российская агрессия привела к углублению сотрудничества ЕС

[46] "EU Supports Cybersecurity in Ukraine with over 10 Million Euro," *Delegation of the European Union to Ukraine*, October 20, 2022, https://www.eeas.europa.eu/delegations/ukraine/eu-supports-cybersecurity-ukraine-over-10-million-euro_en.

[47] "Ukraine and EU Held the Second Round of the UA-EU Cybersecurity Dialogue," *European External Action Service*, September 29, 2022, https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en.

и НАТО при непоколебимой приверженности дальнейшей поддержке Украины, в частности, к созданию совместной координационной группы ЕС-НАТО. Значительный прогресс достигнут в таких областях, как противодействие дезинформации, гибридным и кибер угрозам, терроризму, а также развитие оборонного потенциала, оборонной промышленности и исследований. Тем не менее необходимо и дальше расширять сотрудничество в таких областях, как устойчивость, защита критической инфраструктуры, новые и прорывные технологии, космос, геостратегическая конкуренция, а также более тесное взаимодействие с промышленностью и наукой.[48] Кроме усиления возможностей и устойчивости НАТО, ЕС и отдельных стран-участниц в киберпространстве, цели и задачи также включают подготовку к крупной эскалации в области международной безопасности.

Заключение

Гибридная, а затем и обычная война России с гибридными элементами побудила Европейский Союз развивать возможности организации и стран-участниц в области кибербезопасности и выделить социальную устойчивость как приоритет. Учитывая российскую и китайскую киберкультуру, НАТО признала киберпространство ещё одной сферой ведения войны; следовательно, основная цель Альянса распространяется и на эту сферу. НАТО постоянно развивает оперативные возможности в киберпространстве (например, доктрину кибероперaций) и устойчивость общества, что создаёт ожидания на разных уровнях, стремясь довести осведомленность до гражданского уровня.

В результате этих усилий подход Европейского Союза к кибербезопасности в последние годы также изменился на 180 градусов. Безопасность киберпространства и связанных с ним систем теперь оценивается не так, как 10 лет назад – не только как экономическая проблема, но как проблема, затрагивающая всё общество, существенно влияя на жизнь и жизненное пространство государства, экономики и отдельных людей. Поэтому она требует гораздо более сложной стратегии и регулирования. ЕС также принял меры по снижению киберугроз, возникающих из-за гибридности, включая дезинформацию, что может привести к более эффективному регулированию платформ соцсетей. Однако для достижения этой цели предстоит пройти долгий путь.

Следует также отметить, что человеческое общество во многом взаимосвязано, а количество киберугроз чрезвычайно велико и требует срочного реагирования. Кибератаки очень разнообразны; некоторые из них угрожают территориальной целостности, политической независимости, нацио-

[48] NATO, “Vilnius Summit Communiqué,” issued by NATO Heads of State and Government Participating in the Meeting of the North Atlantic Council in Vilnius, July 11, 2023, points 1, 6, 18, 23, 61, 66, 73, 74, https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

нальной безопасности Союза или стран-участниц настолько, что можно использовать договорные обязательства. Эту точку зрения разделяют Хили и Сингх, которые считают, что, учитывая преобладающие тенденции эскалации напряжённости, будущие действия по деэскалации уже не могут эффективно разрядить напряжённость. Это особенно верно, если отдельные государства рассматривают прошлые инциденты как повод для развития своих возможностей или видят в кибероперациях провокацию. Поэтому наступательные кибероперации с большей вероятностью могут перерасти в открытый вооружённый конфликт, что делает даже умеренные операции значительно более опасными.[49] В докладе Сьюзен Дэвис особенно проблемными названы операции, подрывающие доверие общества в ходе конфликта при помощи киберсредств. Такие операции приводят к более высокой эскалации кризиса, а это означает, что НАТО, ЕС и их страны-участницы должны уделять больше внимания динамике эскалации в своем законодательстве и практике, о чем свидетельствует русско-украинская война.

Учитывая срочность, заинтересованным сторонам необходимо должным образом адаптировать свою киберполитику, уточнив цели и сроки, которые нужно регулярно обновлять. Соответствующим субъектам важно найти должные уровни регулирования и, насколько возможно, согласовать национальные правила, практику и стандарты. ЕС добился существенного прогресса в реализации таких инициатив, как NIS2 и DORA. Однако минимальный уровень внедрения, за который выступают некоторые страны-участницы, по-прежнему приводит к разной скорости регулирования, стандартам и практикам кибербезопасности. Но, как мы знаем, система безопасна настолько, насколько безопасно её самое слабое звено.

Примечание

Представленные здесь взгляды принадлежат исключительно автору и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнёрство ради мира», организаций-участниц или издателей Консорциума.

Об авторе

Д-р Роланд Келемен – юрист, адъюнкт-профессор факультета права и политологии Университета им. Иштвана Сечени. Был стипендиатом программы Фулбрайта в 2021–2022 гг. по программе «Кибербезопасность в университетах – ознакомительные визиты в США».
https://orcid.org/0000-0002-5419-8425
Электронная почта: Kelemen.roland@ga.sze.hu

[49] Jason Healey and Virpratap Vikram Singh, “Situational Cyber Stability and the Future of Escalating Cyber Conflict,” in *Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis*, ed. Pirek Pernik (Tallinn, Estonia: NATO CCDCOE Publications, 2022), 19-31, 29, https://ccdcoe.org/library/publications/cyberspace-strategic-outlook-2030-horizon-scanning-and-analysis/.

Благодарность

Connections: The Quarterly Journal, Vol. 22, 2023, вышел при поддержке правительства США.