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

Ч. Бриггс, Ю. Данык, Т. Малярчук
Connections QJ 20, no. 3-4 (2021): 33-61
https://doi.org/10.11610/Connections.rus.20.3-4.03

Рецензированная статья

Аспекты безопасности гибридной войны, пандемия COVID-19 и кибер-социальные уязвимости

Чэд Бриггс,[1] Юрий Данык,[2] Тамара Малярчук [3]

[1] *Университет Аляски в Анкоридже, https://www.uaa.alaska.edu*

[2] *Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», https://kpi.ua/en/*

[3] *Рабочая группа Программы совершенствования военного образования (DEEP) НАТО, https://deepportal.hq.nato.int/eacademy/*

Аннотация: В то время как развитие кибертехнологий способствовало распространению и росту масштабов гибридных войн, пандемия COVID-19 обострила многие уязвимости и критические зависимости. В этой статье рассмотрены основные цели и стратегии гибридной войны с точки зрения психологической основы и технологического охвата, а также связи с возникающими проблемами дезинформации, киберпреступности, фейковых новостей, информационной травмы и влияния новых форм образования на национальную безопасность и устойчивость государства.

Ключевые слова: гибридная война, кибератака, кибербезопасность, информационная травма, электронное обучение, эмоциональная война, когнитивное хакерство, кибер-социальные уязвимости, кибертехнологии, COVID-19.

Вступление

Концепция гибридной войны привлекает всё больше внимания при обсуждении вопросов безопасности и военной стратегии, часто – на примере действий России по захвату украинского Крымского полуострова в 2014 г. При

комплексном подходе к пониманию наступательных операций, от кампаний в соцсетях до обычной (кинетической) войны, термин «гибридная война» можно применить к широкому спектру действий. Чаще всего акцент делают на нерегулярном характере операций, когда традиционное западное понимание конфликта прикрыто силами и тактикой, которые трудно увязать с враждебным государством. В наших предыдущих статьях мы подробно описали использование кибертехнологий для широкого спектра атак на Украину с 2013 г., включая удары по энергетической инфраструктуре.[1] Для понимания уязвимости стран к утрате контроля за энергоснабжением важна способность противника подорвать доверие общества к институтам: когда основные потребности не удовлетворены, социальные расколы в стране или регионе усугубляются, и управление усложняется.

Ведение гибридных войн во всём мире в настоящее время неоспоримо. Страны от России до Китая на протяжении десятилетий включают идеи войны четвертого поколения в военные доктрины, где «красная линия» между миром и войной размывается, а по отношению к противнику действуют в рамках общей стратегии асимметричного, теневого (скрытого) конфликта.[2] Это не во́йны в традиционном смысле Гаагской или Женевской конвенций с чётким началом и концом, физической оккупацией территории, видимыми участниками и ясными намерениями. Гибридные войны пересекают границы и могут вестись постоянно, иногда – с нападением на целые страны, а иногда в отношении конкретных групп или людей. Но действия гибридной войны всегда имеют цель и мобилизуют ресурсы для её достижения. Все остальное — лишь инструмент достижения этой цели в интересах конкретных игроков (субъектов). Важным элементом тут является комплексная стратегия игрока, направленная на то, чтобы вывести другого игрока из равновесия, дестабилизировать его настолько, чтобы вскрыть стратегическое пространство для политических, экономических и военных действий.[3]

Гибридные войны – это вид постоянной войны разной интенсивности во многих сферах, с каскадными негативными последствиями и синергетическими эффектами, в которые в какой-то мере, сознательно или неосознанно, вовлечено всё население страны и международное сообщество. Их последствия ощущаются во всех сферах жизни, во всех слоях общества и по всему государству. Использование инновационных технологий позволило сместить конфликт с преимущественно открытых и силовых (кинетических)

---

1 Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs, “Hybrid War: High-tech, Information and Cyber Conflicts,” *Connections: The Quarterly Journal* 16, no. 2 (2017): 5-24, https://doi.org/10.11610/Connections.16.2.01.

2 Robert Wilkie, “Hybrid Warfare: Something Old, Not Something New,” *Air & Space Power Journal* 23, no. 4 (Winter 2009): 13-18.

3 Daniel T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory* (FT Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2009), https://apps.dtic.mil/sti/pdfs/ADA513663.pdf.

средств на менее очевидные стратегии, нацеленные на структурные уязвимости противников, в том числе за счёт достижения когнитивного преимущества и контроля над ними.

Такая гибридная тактика позволяет взять под контроль или дестабилизировать основные институты страны и достичь стратегических интересов нетрадиционным кибер- и когнитивным воздействием (с побочными эффектами). Основным театром асимметричных действий стало киберпространство, в силу того, что киберпространство имеет экстерриториальный, универсальный и глобальный характер. Оно также мало соотносится с географическими границами стран, может служить средой общения для людей почти всех возрастов и постоянно расширяется в масштабах и влиянии. Информационные потоки могут быть реализованы посредством диалога с массовой аудиторией и с использованием соцсетей для достижения или имитации индивидуального общения. На данный момент кибертехнологии стали важнейшим инструментом формирования коллективного и индивидуального сознания и ценностей общества.

Таким образом, кибертехнологии позволяют применять гибридные стратегии для достижения целей широкомасштабного воздействия на общество на расстоянии без возможности однозначно идентифицировать агрессора. Наиболее эффективные пользователи кибер-гибридных подходов выбирают конечные цели, которых нужно достичь, и выстраивают соответствующий набор синергетических действий с перекрывающимся, каскадным и усиливающим воздействием. Эти действия направлены на выведение из строя противника, продвижение заранее подготовленных нарративов и контроль когнитивной сферы на эмоциональном, моральном, культурном и ментальном уровнях. Успешные действия могут создать систему устойчивых стереотипов и восприятия действительности или же просто способствовать нестабильности и отрицанию объективных стандартов и истины.

Пандемия COVID-19, бушевавшая на планете с декабря 2019 г., добавила новые черты к спектру гибридных противостояний и методов. Их необходимо учитывать при анализе и прогнозировании для снижения рисков и предотвращения и/или смягчения последствий. Данная статья посвящена социальной природе гибридной войны и технологическим возможностям использования социальной и политической уязвимости и поляризации в подвергшихся нападению государствах. Эти вопросы рассмотрены в контексте гибридной войны, пандемии COVID-19 и возникающих кибер-социальных уязвимостей.

При всей важности внимания к военной и физической инфраструктуре гибридных атак, такие наступательные операции используют хрупкие социальные и политические структуры, являющиеся неотъемлемым элементом планирования наступательных стратегий и, соответственно, защиты от гибридных атак. Исторический опыт показал, что действия гибридной войны в этой сфере выгодны атакующему – хотя такие страны, как США, и ранее

использовали гибридные методы для усиления политической поддержки в зонах конфликтов, чаще успешно (например, Филиппины в 1950-х гг.), чем провально (Ирак после 2003 г. или Афганистан).[4] Там, где агрессор хорошо знает своего противника, общественные разногласия легко использовать, и они гораздо более уязвимы при умелом использовании киберинструментов, таких как социальные сети. На примере Украины и США в этой статье подробно описаны методы применения технологий асимметричного подхода для влияния и подрыва управления противника.

Идея атаковать социальную структуру противника не нова. Ещё Сунь-Цзы говорил о подрыве морального духа противника и предупреждал, что затяжной конфликт снизит поддержку войны обществом.[5] Клаузевиц тоже отмечал политическую природу войны, понимая, что победы в сражении может быть недостаточно, чтобы выиграть войну в целом.[6] Эксперты по борьбе с повстанцами и нерегулярной войне в XX веке ещё больше отмечали важность морального духа общества вне традиционного поля боя и указывали, что прямая военная сила может оказаться контрпродуктивной для завоевания политической поддержки в конфликте. Показательным примером стали дебаты по поводу стратегических бомбардировок ВВС США, особенно по гражданским целям во время Второй мировой войны в Европе. Официально имея промышленные и военные цели, американские бомбардировки с больших высот в Европе часто приводили к большим жертвам среди гражданского населения, при этом выдвигался аргумент (особенно в Королевских ВВС) о том, что разрушение городов подорвёт моральный дух общества и поддержку немецкой агрессии против Запада.[7] Немецкие «Люфтваффе» приводили аналогичные аргументы в пользу бомбардировок Великобритании в 1940-41 гг., со столь же разочаровывающими результатами.[8] Вместо того, чтобы подорвать моральный дух немцев или британцев, видящих, как разрушают их города, а соседи гибнут в результате бомбардировок, общество обычно сплачивалось в поддержку государства в ответ на такую открытую агрессию.

Аналогичным образом, десятилетия спустя, военные действия США против вьетнамских деревень, подозреваемых в укрытии партизан Вьетконга,

---

4 Ivan Arreguin-Toft, “How to Lose a War on Terror: A Comparative Analysis of a Counterinsurgency Success and Failure,” in *Understanding Victory and Defeat in Contemporary War*, ed. Jan Angstrom and Isabelle Duyvesteyn (Routledge, 2006), 160-185.

5 Sun Tzu, “The Art of War,” in *Strategic Studies: A Reader*, ed. Thomas G. Mahnken and Joseph A. Maiolo (Routledge, 2014), 86-110.

6 Carl von Clausewitz, *On War* (Penguin UK, 1982).

7 Kenneth P. Werrell, “The Strategic Bombing of Germany in World War II: Costs and Accomplishments,” *The Journal of American History* 73, no. 3 (December 1986): 702-713, https://doi.org/10.2307/1902984.

8 Edgar Jones, Robin Woolven, Bill Durodié, and Simon Wessely, “Civilian Morale During the Second World War: Responses to Air Raids Re-examined,” *Social History of Medicine* 17, no. 3 (2004): 463-479, https://doi.org/10.1093/shm/17.3.463.

казалось, лишь усилили поддержку Вьетконга или по крайней мере настроили общественное мнение против американцев.[9] Карр утверждал, что открытое насилие против гражданского населения (в отличие от военных), будь то со стороны американских военных во Вьетнаме или Ирландской республиканской армии в Великобритании/ Ирландии, вело к пониманию незаконности этих действий и утрате народной поддержки.[10] Но ключевым элементом таких оценок была очевидность таких действий и их ясные намерения. В тех же случаях, когда в агрессивных действиях можно было обвинить других (нападения под чужим флагом) или когда характер нападения не включал физического насилия, установить виновных и обвинить кого-либо очень сложно.

Разделённый дом

Российские военные давно признали важность асимметричных подходов к военному конфликту, то есть использования уязвимых мест противника, непропорциональное имеющимся силам. Обычный подход России – проведение операций влияния, действий, не достигающих порога военного реагирования в западных странах, которые можно скрыть, не признавая своих агрессивных действий или намерений. Операции влияния предполагают использование в основном непрямых и некинетических средств для раздора и раскола у противника, используя уже имеющиеся внутренние/ внешние силы для поляризации политики, делегитимизации правительства и его институтов, а также подрыва стойкости населения и общества при реагировании на внешние угрозы.[11] Хотя история операций влияния не нова, кибертехнологии позволили эффективно проникать из любой точки мира прямо в компьютеры и телефоны людей, маскируя при этом истинный источник информации или дезинформации.

В некоторых военных стратегиях, включая стратегии Российской Федерации и Китая, немало внимания уделено информационным операциям как элементу более крупных стратегий и операций, а не отдельным операциям, как это часто бывает в США и Западной Европе. Независимо от того, называют ли их частью «революции в военном деле» или других доктрин, на практике эти стратегии относятся к асимметричным и информационно-ориентированным активным мерам против противника. Как отмечал Госдепар-

---

[9] Richard Shultz, "Breaking the Will of the Enemy During the Vietnam War: The Operationalization of the Cost-Benefit Model of Counterinsurgency Warfare," *Journal of Peace Research* 15, no. 2 (June 1978): 109-129, https://doi.org/10.1177/002234337801500202.

[10] Caleb Carr, *The Lessons of Terror: A History of Warfare Against Civilians* (New York: Random House, 2003).

[11] Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," *Russia Report* 1 (Washington, D.C.: Institute for the Study of War, September 2015).

тамент США в 1989 г. в отношении действий СССР, «активные меры» означают сочетание дезинформации и фейков, подставных групп, оппозиционных партий и операций политического влияния. Всё это использовалось для маскировки войны под видом безобидных действий.[12]

Бэгги описывал концепцию рефлексивного контроля в российской стратегии так: «Рефлексивный контроль служит для разрушения самой системы принятия решений, чтобы заставить её работать в интересах агрессора и, таким образом, установить власть без привлечения серьёзных военных или политических ресурсов, не превышая признанного порога вмешательства в международные дела суверенной страны».[13] Рефлексивный контроль является развитием советской военной доктрины, где особое внимание уделялось нарушению процессов принятия решений противником и дезинформации с тем, чтобы противник реагировал так, как выгодно для Советов (русских). Если командир противника чувствует, что его выбор ограничен определёнными вариантами, успешный рефлексивный контроль возникает, когда эти варианты способствуют стратегии России, и решение легче предвидеть.

В совокупности гибридная война, в понимании российского правительства и военных, предполагает целостную стратегию подрыва и дестабилизации противника, применяя широкий спектр средств, но (по возможности) используя слабости врага в интересах российской стратегии. В конечном счёте концепция рефлексивного контроля заключалась в том, чтобы влиять на информацию, доступную военным, ведя их по заранее определённому (русскими) пути, который можно было спланировать и который позволил бы России использовать свои сильные стороны в боевых действиях. Хотя это трудно в полной мере реализовать в традиционной войне (британские военные и разведслужбы исторически были успешнее других в стратегической дезориентации противника), кибертехнологии повышают возможности дезинформации. Успех позволит не только расколоть общество, подвергшееся нападению, но и заставит сами «мишени» распространять дезинформацию и негативные нарративы.

Когнитивное хакерство

Применяя новые развивающиеся технологии, злоумышленники всё чаще используют психологические приемы и манипуляции в когнитивном пространстве. Эти тактики часто повторяют хакерские (фишинг, спуфинг и т.д.) и представляют собой особый тип социальной инженерии. Их применение увеличивает возможность несанкционированного доступа к информационным ресурсам в киберпространстве, важным для когнитивной сферы общества, с возможностью деструктивного воздействия на неё. Это явление

[12] Daniel P. Bagge, *Unmasking Maskirovka: Russia's Cyber Influence Operations* (Washington, DC: Defense Press, February 2019).

[13] Bagge, *Unmasking Maskirovka*.

называют «когнитивным хакерством».[14] В его основе лежит манипулирование общественным сознанием в киберпространстве – не только с целью кражи денег или данных, но и чтобы повлиять на поведение пользователей, навязать им свою волю и контролировать их. Практически любой пользователь киберпространства может заниматься когнитивным хакерством в виде дезинформации, манипулирования репутацией и/или распространения на интернет-платформах контента, меняющего восприятие реальности у других пользователей. Оно может принимать форму кибератак, кибердействий и операций, направленных на манипулирование человеческим восприятием реальности с использованием уязвимостей обработки информации людьми и соцсетями. Такие атаки направлены на изменение поведения, восприятия или отношения людей к значимым событиям или темам, таким, как пандемия COVID-19, и преследуют конкретную цель.[15]

В 2019 г. количество фишинговых атак (создание фейковых сайтов или ссылок, имитирующих сайты известных компаний) выросло на 400 %. При этом более 24 % адресов вредоносных страниц (URL) располагались на легитимных доменах, используя доверие к ним пользователей, а фишинг стал более персонализированным, включая отслеживание присутствия и активности конкретного пользователя в киберпространстве.[16] Помимо фишинга, киберпреступники используют спуфинг (маскировку вредоносной программы под легальную) для политических атак. Так, в марте 2016 г. высокопоставленный чиновник предвыборного штаба Хиллари Клинтон, Джон Подеста, ввёл свои учетные данные на странице, не распознав фейковое уведомление, якобы полученное от Google. Так произошёл взлом, и злоумышленники получили доступ к его данным, которыми затем воспользовались иностранные и местные политики.[17]

Эмоциональная война

В более сумрачном, некинетическом спектре гибридной войны контроль над информацией нацелен не только на когнитивные процессы, но и на

---

[14] Darren L. Linvill et al. "'The Russians Are Hacking My Brain!' Investigating Russia's Internet Research Agency Twitter Tactics During the 2016 United States Presidential Campaign," *Computers in Human Behavior* 99 (October 2019): 292-300, https://doi.org/10.1016/j.chb.2019.05.027.

[15] Ian Baxter, "The Cognitive Psychological Tricks Hackers Use to Dupe Users," *ITProPortal*, March 12, 2020, www.itproportal.com/features/the-cognitive-psychological-tricks-hackers-use-to-dupe-users.

[16] Muhammad Adil, Rahim Khan, and M. Ahmad Nawaz Ul Ghani, "Preventive Techniques of Phishing Attacks in Networks," in *Proceedings of the 3rd International Conference on Advancements in Computational Sciences*, ICACS 2020, Lahore, Pakistan, February 17-19, 2020 (IEEE, 2020), 1-8, ISBN 978-1-7281-4235-7.

[17] Travis Farral, "Nation-state Attacks: Practical Defences against Advanced Adversaries," *Network Security* 2017, no. 9 (September 2017): 5-7, https://doi.org/10.1016/S1353-4858(17)30111-3.

лимбические, эмоциональные центры мозга.[18] Людям присуще делить мир на различные категории идентичности, чтобы понять смысл сложного мира и объяснить причины происходящего. Политические психологи уже давно показали, что эти категории не обязательно должны иметь какую-то внутреннюю ценность. Они могут быть совершенно произвольны, основываться на мифах, или быть усвоены от авторитетов, например, путём разделения школьников на случайные группы по цвету глаз, или национальные категории, основанные на исторических событиях, имевших место столетия назад. Посторонним такое разделение может показаться случайным, как в сатире Джонатана Свифта на различия между католиками и протестантами в 1723 г. Тем не менее в соцсетях это разделение может выглядеть реальным и подкрепляться политической, экономической и медийной практикой.

Психологи определили траектории, по которым разделение на «своих» и «чужих» может перерасти из социально приемлемых различий в потенциально жестокие и трудноразрешимые антагонизмы. Во-первых, различия делают существенными или характерными, то есть на группу налагают широкие стереотипы, объясняющие, что социальные (расовые, языковые, религиозные и т.д.) различия являются важными чертами этой группы. Если человек рождается или воспитывается в такой группе, эти различия считаются устоявшимися, и их нелегко изменить. Затем «чужих» обесценивают в соответствии с этими чертами, а образы и истории в СМИ часто толкуют так, чтобы усилить эти негативные стереотипы.[19] Первые два процесса часто способствуют повышению оценки своей группы, подчеркивая отличия в том, что делает человека «хорошим». Американский патриотизм на протяжении всей холодной войны часто основывался на различии между «трудолюбивыми американцами» и «неэффективными, безбожными коммунистами», в то время как другие националисты будут стараться подчеркнуть превосходство своей культуры над другими.[20]

Более опасные процессы происходят, когда потребности общества не удовлетворены или не могут быть удовлетворены, от базовых потребностей, таких, как дорогая еда, до более экзистенциальных угроз утраты культуры или престижа. Когда в обществе открыто или скрыто присутствуют та-

---

[18] Linton Wells II, “Cognitive-Emotional Conflict: Adversary Will and Social Resilience,” *Prism* 7, no. 2 (December 2017): 4-17, https://cco.ndu.edu/PRISM-7-2/Article/1401814/cognitive-emotional-conflict-adversary-will-and-social-resilience. Мы также благодарны Александре Несич за её работу об эмоциональной войне.

[19] Marilynn B. Brewer, “The Psychology of Prejudice: Ingroup Love and Outgroup Hate?” *Journal of Social Issues* 55, no. 3 (Fall 1999): 429-444, https://doi.org/10.1111/0022-4537.00126.

[20] Robert T. Schatz, Ervin Staub, and Howard Lavine, “On the Varieties of National Attachment: Blind Versus Constructive Patriotism,” *Political Psychology* 20, no. 1 (March 1999): 151-174, https://doi.org/10.1111/0162-895X.00140. Следует отметить, что некоторые виды национализма по своей природе негативны, концентрируясь на исторических поражениях и ощущении жертвы.

кие страхи, возникает возможность приписать эти угрозы сторонним группам. Исторически антисемитизм часто основывался на том, что евреев обвиняли в финансовых проблемах большинства населения, исходя из стереотипа об их исторической социальной роли банкиров, юристов и ученых. Дегуманизация и/или деполитизация групп в сочетании с виной за неспособность общества достичь основных целей или потребностей опирается на предполагаемые существенные характеристики группы, чтобы поляризовать мнения и согласиться с насильственными средствами защиты от угроз извне.[21]

Пропагандистские кампании во время войны часто использовали такие стратегии, будь то стереотипы Первой мировой о немецких «гуннах», убивающих невинных женщин и детей, или агитация в США против якобы фанатизма и бесчеловечности японцев.[22] Но самые крайние проявления возникали, когда дегуманизация группы принимала такие масштабы, что геноцид принимался и поощрялся, как, например, в отношении евреев во время Второй мировой войны, мусульман в Боснии и Герцеговине или «нежелательных элементов» в Камбодже при Красных кхмерах.[23] Но открытая война и оправдание геноцида не всегда сопровождают раскол в обществе, как критический элемент конфликта. Модель гибридной войны не предполагает массового насилия против населения, предпочитая использовать раскол у противника против него самого.

США: Познай себя

Разведка США предупреждала о вмешательстве России в американскую политику как минимум с 2016 г. В недавнем докладе Мюллера указано, что серьёзные попытки России повлиять на выборы начались не позднее 2014 г. Это было совсем не то, что некоторые критики пренебрежительно называют «несколькими рекламными объявлениями в Facebook»: усилия России (как кибер-, так и человеческие) вылились в скоординированную кампанию по подрыву доверия к институтам США, усилению политической неуверенности и поляризации.[24] Отсутствие окончательного вердикта об эффекте таких

---

[21] Ervin Staub, “The Roots of Evil: Social Conditions, Culture, Personality, and Basic Human Needs,” *Personality and Social Psychology Review* 3, no. 3 (1999): 179-192, https://doi.org/10.1207/s15327957pspr0303_2.

[22] Harold D. Lasswell, *Propaganda Technique in the World War* (Ravenio Books, November 2015).

[23] Michał Bilewicz and Johanna Ray Vollhardt, “Evil Transformations: Social-Psychological Processes Underlying Genocide and Mass Killing,” *Social Psychology of Social Problems: The Intergroup Context*, ed. Agnieszka Golec de Zavala and Aleksandra Cichocka (New York, NY: Palgrave Macmillan, 2012): 280, https://doi.org/10.1007/978-1-137-27222-5_11.

[24] Robert S. Mueller, “Report on the Investigation into Russian Interference in the 2016 Presidential Election,” The Final Report of the Special Counsel into Donald Trump, Russia, and Collusion (Washington, D.C.: US Department of Justice, March 2019), https://www.justice.gov/archives/sco/file/1373816/download.

действий на выборах 2016 г. не имеет значения: если цель заключалась в усилении неуверенности и подрыве доверия, то сама постановка таких вопросов уже говорит о достижении главной цели.

США во многих отношениях были и остаются уязвимыми для кибероперациий гибридной войны ещё до событий 6 января 2021 г. Это страна с глубокими политическими, экономическими, региональными, расовыми и гендерными различиями. Большинство американских политиков не подчёркивают различий, кроме партийных, предпочитая вместо этого говорить об общих политических устремлениях американцев. Тем не менее существовала возможность использовать скрытые разногласия и недовольство, а такие киберинструменты, как социальные сети, обеспечили беспрепятственный доступ к миллионам американцев. Проводимая российским ГРУ и «Лахтой» (Агентством интернет-исследований) целенаправленная кампания была направлена на поляризацию американцев по таким разделяющим общество вопросам, как иммиграция, гендерные права и религия. В рассекреченном отчёте разведки США от января 2017 г. резюмируется: «Мы считаем, что президент России Владимир Путин приказал в 2016 г. провести кампанию влияния на президентские выборы в США. Целью России было подорвать веру общества в демократический процесс в США, очернить госсекретаря Клинтон и помешать её избранию и возможному президентству. Мы также считаем, что Путин и российское правительство явно отдают предпочтение избранному президенту Трампу. Мы вполне уверены в этих оценках».[25]

Считают, что поскольку Клинтон была фаворитом на выборах, действия России могли помешать её президентству, посеяв сомнения в его легитимности. Предпринятые кибердействия включали взлом электронной почты партий (как демократов, так и республиканцев), киберагрессию – публикацию избранных сообщений в изменённом виде в таких источниках, как Wikileaks, создание псевдообщественных политических групп в соцсетях, подставных аккаунтов в сетях Facebook и Твиттер, выдающих себя за избирателей США, организацию надуманных протестов и контрпротестов, создание и распространение фейковых и лживых новостных сообщений, нацеленных в основном на избранные группы населения в ключевых штатах. Использование метаданных социальных сетей очень упростило процесс: пользователи, использовавшие ключевые слова, например, с беспокойством по поводу иммиграции мусульман, могли получать рекламу и политические сообщения, усиливающие такие опасения по отношению к определённым кандидатам.[26]

Хотя тактика России часто имела успех, её можно применить только в

[25] Bill Priestap, “Assessing Russian Activities and Intentions in Recent US Elections,” Unclassified Intelligence Community Assessment (Office of the Director of National Intelligence, January 2017), p. ii.

[26] Philip N. Howard et al., “The IRA, Social Media and Political Polarization in the United States, 2012-2018” (University of Oxford, 2018).

политическом ландшафте, где уже существуют значительные разногласия, фейковые новости и теории заговора могут найти отклик у значительной части населения, а технологии достаточно распространены – по меньшей мере 30 миллионов американцев могли получать российские сообщения.[27] Вместо того, чтобы ощутить себя американцами, совместно противостоящими действиям России, люди в США нападали друг на друга, разделившись на «своих» и «чужих», используя выражения наподобие «настоящие американцы» и говоря о патриотизме. «Лахтоботы» не ограничилась выборами, а активно участвовали в антинаучных кампаниях, особенно по вопросам изменения климата и против вакцинации. Их содействие распространению таких дремлющих болезней, как корь (к весне 2019 г. некоторые штаты США объявили чрезвычайное положение из-за её вспышек), нельзя объяснить одними лишь действиями России, но они имели целью вывести на поверхность подводные течения, уже имевшиеся в американском обществе,[28] «прыгая» по существующим темам, «критичным» для общества или отдельных целевых групп.

Пандемия COVID-19 высветила многие из этих различий: разногласия использовали или провоцировали в ответ на меры здравоохранения. В протестах против вакцин от COVID в 2021 г. участвовали и левые, и правые, при этом использование масок от коронавируса было связано с линией партии.[29] Многие хотели раздуть пожар, не соглашаясь с происхождением и смертоносной природой вируса; подобные стереотипы окутывали различные споры, чаще политические, чем медицинские. Общая стратегия России и Китая заключалась в том, чтобы зародить сомнения в эффективности реакции демократических институтов на пандемию.[30]

Политическая психология разделения на «своих» и «чужих» помогает понять, что когда эти разногласия усилены средствами массовой информации и политическими нарративами, разделение становится гораздо более резким как для сторонних наблюдателей, так и для тех, кто относит себя к тому или иному лагерю. Это не только крайне усложнило традиционное двухпартийное законотворчество и управление на федеральном уровне, но и усилило разногласия. Когда появляется новая дезинформация (или пред-

---

[27] Howard et al., “The IRA, Social Media and Political Polarization.”

[28] David A. Broniatowski et al., “Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate,” *American Journal of Public Health* 108, no. 10 (October 2018): 1378-1384, https://doi.org/10.2105/AJPH.2018.304567; Shanta Barley, “Climategate: Russian Secret Service Blamed for Hack,” *New Scientist* 7 (2009).

[29] Rose Bernard, Gemma Bowsher, Richard Sullivan, and Fawzia Gibson-Fall, “Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare,” *Health Security* 19, no. 1 (2021): 3-12, https://doi.org/10.1089/hs.2020.0038.

[30] Sergey Sukhankin, “COVID-19 as a Tool of Information Confrontation: Russia’s Approach,” *The School of Public Policy Publications* 13, no. 3 (April 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3566689.

взятый целевой контент запускает заранее определённые (спланированные) процессы или идеи), независимо от первоисточника, американцы могут делиться такой информацией в соцсетях, а алгоритмы отбора (например, через Facebook) ещё больше укрепляют мысль о том, что этой информации можно доверять, потому что ею поделился заслуживающий доверия американец. В то время как советской пропаганде в 1970-х – 1980-х гг. приходилось целенаправленно работать над отмыванием источников по нескольким фронтам, с помощью киберинструментов сообщение или нарратив можно вбросить и распространить без особых усилий, если они отражают то, что люди хотят или ожидают увидеть.

Технологии социальных сетей – не исключение. Эффективная гибридная война использует различные инструменты для достижения цели разрушения или контроля. Атаки на энергетическую инфраструктуру были отмечены и в США, при чём правительство США признало, что атаки типа «отказ в обслуживании» нарушили работу электросетей на западе США в марте 2019 г. После того, как стало известно о возможности таких атак, и что попытки взлома уже предпринимались ранее, стало понятно, что США могут реально пострадать от сбоев в работе критических служб, как это ранее было в Украине (которая, в некотором смысле, стала испытательным полигоном для технологий будущих войн, включая кибернетические, информационные и когнитивные действия). Стратегическая цель таких угроз или действий – создать ощущение неуверенности и незащищённости, отвлечь граждан и руководителей, заставив их думать о том, как интерпретировать события и информацию.

Полагают, что события в США находятся на гораздо более низкой ступени эскалации, чем в других странах (например, в Грузии, Эстонии, Украине, Сирии). Тем не менее важно ещё раз подчеркнуть, что не существует «красной линии», которая отличала бы стратегии гибридной войны в одной стране от другой. Цели различаются по степени желаемой дестабилизации с учетом того, что может вызвать активный ответ государству-агрессору. Опыт США показал, что постепенные и скрытые действия могут со временем снизить порог реагирования, допуская большее вмешательство и дестабилизацию при отсутствии сильной скоординированной защиты.[31]

Пожар на Востоке

Нынешний конфликт в Украине часто приводят в качестве одного из главных примеров гибридной войны последних лет, хотя многие аналитики прежде всего вспомнят об оккупации Крыма в 2014 г. Открытый конфликт в Донецкой и Луганской областях с середины 2014 г. привлекает меньше внимания,

[31] Rubén Arcos, Manuel Gertrudix, Cristina Arribas, and Monica Cardarilli, “Responses to Digital Disinformation as Part of Hybrid Threats: A Systematic Review on the Effects of Disinformation and the Effectiveness of Fact-checking/Debunking,” *Open Research Europe* 2, no. 8 (2022), https://doi.org/10.12688/openreseurope.14088.1.

а в западных СМИ его часто ошибочно называют «гражданской войной». Даже когда анализ насильственного конфликта на востоке включает сбитие рейса МН-17 Малайзийских авиалиний в июле 2014 г., эти насильственные действия представляют собой лишь наиболее видимые аспекты гибридной войны.[32] Этот конфликт имеет ряд характерных черт, наиболее примечательной из которых является появление свидетельств того, что некинетическая (т.е. информационная) война оказывает существенное травмирующее воздействие на общество вдали от линии фронта на востоке Украины.

Деструктивные действия концентрируются на критических узлах социальных и связанных с ними систем, уязвимостях, которые можно использовать, а затем переходят в самоподдерживающийся нисходящий цикл повторяющихся шагов и воздействий (в научных терминах – петли положительной обратной связи). Но поскольку целевые узлы разнесены по географическим и функциональным зонам, стороннему наблюдателю может быть трудно увидеть характер предполагаемых воздействий и общую стратегию агрессора. Для стратегий национальной безопасности важно уметь выявлять такие рассредоточенные и тайные действия и противостоять им, а также понимать сложные каскадные последствия агрессивных действий, которые не приводят в действие традиционную концепцию «актов войны».

Как и для других сложных систем безопасности, таких, как энергетика или окружающая среда, часто критичней всего не первоначальное воздействие, а эффекты второго и третьего порядка, возникающие в результате первоначального нарушения. Поначалу может быть трудно увидеть причинно-следственную связь событий, а неправильные ответные меры могут усугубить цепочки последствий.[33] Так, реакция советского руководства на катастрофу на Чернобыльской АЭС в 1986 г. стала, пожалуй, одним из худших примеров реагирования. Тогда политические соображения привели к облучению десятков тысяч граждан в Украине и за её пределами. Подобная неадекватная реакция на изменившиеся условия легко может усугубить другие бедствия или конфликты.[34] Следуя принципам рефлексивного контроля, эффективная кампания гибридной войны может завести правительство в петлю положительной обратной связи с ухудшающимися последствиями второго и третьего порядка.

Гибридная война в Украине показала стратегическую важность плановых скоординированных действий и необходимые компоненты в киберсфере:

- Конечные цели, которые должны быть достигнуты;

---

[32] Irina Khaldarova and Mervi Pantti, “Fake News: The Narrative Battle over the Ukrainian Conflict,” *Journalism Practice* 10, no. 7 (2016): 891-901, https://doi.org/10.1080/17512786.2016.1163237.

[33] Aura Reggiani, “Network Resilience for Transport Security: Some Methodological Considerations,” *Transport Policy* 28, no. C (2013): 63-68, https://doi.org/10.1016/j.tranpol.2012.09.007.

[34] Andrew Leatherbarrow, *Chernobyl 01:23:40: The Incredible True Story of the World’s Worst Nuclear Disaster* (Lancaster, UK: Andrew Leatherbarrow, 2016).

- Стратегия ведения кампании;
- Организация кампании;
- Используемая тактика и инструменты;
- Оценка первичного, вторичного и третичного воздействия;
- Оценка и усугубление последствий.

Кибердействия могут вестись последовательно, одновременно, параллельно, рассредоточено или целенаправленно. Рассредоточенные кибердействия направлены на наиболее уязвимые элементы (объекты) инфраструктуры. Совокупность одновременных и/или последовательных кибервоздействий обеспечивает синергетический эффект на непредсказуемые места (элементы, системы, сферы), которые могут быть административно или политически отделены от главной цели, но функционально влияют на критические системы. Вот пример из мира, не связанного с кибербезопасностью: в 2001 г. произошла серия атак сибирской язвы на политиков через почтовую систему США, и в результате пришлось закрыть все почтовые отделения в Вашингтоне. Неожиданным (для специалистов по стихийным бедствиям) результатом стало то, что не были получены чеки об оплате местной коммунальной компании PEPCO, и энергокомпании пришлось обратиться в Белый дом с просьбой о финансировании, чтобы не отключать энергоснабжение столицы США.[35] Кибердействия могут иметь больше прямых последствий в тесно взаимосвязанном мире, где компании надеются на электронные платежи и своевременные поставки товаров и комплектующих. Так, кибератаки Petya в Украине в июне 2017 г. имели побочные эффекты в европейской и мировой финансовой системах, хотя основной целью было украинское государство и компании этой страны в канун национального праздника.[36]

Хотя атаки Petya в 2017 г. встретили эффективный отпор украинских кибервойск, предполагаемые цели в виде финансовых учреждений быстро перекинулись на больницы и страховые компании по всему миру. Эти методы применяют, планируя кибервоздействие с широкими цепными последствиями. Они создают разрушительную волну на взаимосвязанных объектах и системах, одновременно воздействуя на множество пересекающихся сфер. Кибератаки могут проводиться синхронно или асинхронно, параллельно по нескольким линиям атаки или последовательно несколько раз на одном и том же целевом кластере. Ущерб целевым объектам наибо-

[35] Reshma Pradhan Lensing, “Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events,” PhD Dissertation (Massachusetts Institute of Technology, 2003).

[36] Jagmeet S. Aidan, Harsh K. Verma, and Lalit K. Awasthi, “Comprehensive Survey on Petya Ransomware Attack,” In *Proceedings of the 2017 International Conference on Next Generation Computing and Information Systems* (ICNGCIS), IEEE, pp. 122-125.

лее разрушителен и эффективен по критериям «эффективность-время-затраты», хотя некоторые цели могут служить для демонстрации возможностей концепции другим странам, которые могут быть атакованы. Исследования и анализ боевых действий показывают, что действия, связанные с кибербезопасностью, и информационная война становятся всё более масштабными и важными для военных.[37] В этой связи, гибридная война и применение киберсредств в ней относятся к наиболее важным факторам для понимания дуги будущих конфликтов.

Кибератака России на электростанции «Прикарпатьеобленерго» в декабре 2015 г. потребовала месяцев тщательной подготовки и внедрения, а подача электроэнергии была нарушена менее чем на сутки. Но настоящей целью атаки могла быть не только Украина. Атака могла стать проверкой новых методов гибридной войны и предупреждением для других стран, чьи энергосистемы могут быть уязвимы для подобной тактики. Новые кибератаки 2021 и начала 2022 гг. подтверждают, что в Украине идёт настоящая информационная и кибернетическая война, включающая весь спектр деструктивного воздействия как на техническую инфраструктуру, так и на общество. Использование соцсетей для кибератак ещё более выгодно, поскольку они используют собственные алгоритмы систем для распространения дезинформации или нужных нарративов. Миллионы людей можно охватить относительно небольшими усилиями, а в сочетании с кибердарами по другим местам (учреждениям, инфраструктуре) социальные последствия могут резко усилиться.[38]

Гибридная форма коллективной травмы

Хаотичный фон непонимания будущих рисков безопасности в стране, восприятия информации, незнание, кому доверять и можно ли надеяться на основные услуги и институты, усугублённые гибридной войной, могут привести к распространению когнитивного резонанса, диссонанса или дисбаланса. Помимо смятения, описываемого когнитивной психологией, люди могут получить травмы в виде биологических и неврологических патологий, индивидуальную и коллективную психику выталкивают за рамки нормального восприятия, а понимание и доверие искажается, в той или иной степени.[39] Исследования в Украине позволили оценить последствия травм в

[37] Iskren Ivanov and Velizar Shalamanov, “NATO and Partner Countries Cooperation in Countering Asymmetric and Hybrid Threats in South Eastern Europe’s Cyberspace,” in *Toward Effective Cyber Defense in Accordance with the Rules of Law* 149, ed. Alan Brill, Kristina Misheva, and Metodi Hadji-Janev (2020): 59-70, https://doi.org/10.3233/NHSDP200041.

[38] Kim Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid,” *Wired*, March 3, 2016, www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

[39] Jack Saul, *Collective Trauma, Collective Healing: Promoting Community Resilience in the Aftermath of Disaster* 48 (Routledge, 2013).

районах открытого конфликта на востоке. Последние исследования показывают, что «синдром гибридной войны» сильнее, когда вся территория является зоной активного деструктивного воздействия на индивидуальную и общественную психику.

Последствия гибридной войны не ограничиваются числом погибших, искалеченных и пропавших без вести. Они также включают воздействие на когнитивную сферу граждан, сообществ и всего общества. Гибридная война прямо и косвенно влияет на сознание и подсознание, на психофизиологическое, психическое состояние и общественное здоровье участников и очевидцев конфликта. Но в кибермире гибридного конфликта свидетели живут не только в «горячих зонах» кинетической войны. Всё население является свидетелем конфликта и объектом кампаний по подрыву традиционных концепций идентичности, доверия и объективной реальности. В предыдущих конфликтах травму получали те, кто находился в географически определённой зоне боевых действий или там, где средства массовой информации могли транслировать тревожные образы войны в домах людей. Киберинструменты позволяют расширить охват, стирая старые геопространственные границы и односторонний поток информации. Таким образом, и комбатанты, и гражданское население оказываются в зоне гибридного конфликта, что проявляется в ряде психологических и поведенческих характеристик, которые можно в совокупности обозначить как «синдром гибридной войны» и его производные, «военный синдром гибридной войны», «специфическое посттравматическое стрессовое расстройство гибридной войны» и т.д.[40]

В странах, переживающих затяжной конфликт, у определённого слоя населения развился «военный синдром гибридной войны». Этот синдром объясняется боевыми (военными) действиями низкой интенсивности при гибридном конфликте и широким спектром нетрадиционных параллельных воздействий. У тех, кто особенно подвержен насилию в зоне конфликта, часто развиваются серьёзные изменения в индивидуальной психологии и реакции на окружающих, особенно когда они возвращаются из зоны конфликта и испытывают сильный когнитивный диссонанс и отчуждение.[41] Такие люди могут обладать боевыми навыками, неприменимыми в гражданской жизни, и испытывать чрезмерное восприятие угрозы (включая потен-

[40] Yuriy Danyk and Oleksandra Zborovska, “Development and Implementation of a New Concept of Crisis Situations Syndrome: ‘Syndrome of a Hybrid War’,” *EUREKA: Health Sciences* 6 (2018): 15-29, https://doi.org/10.21303/2504-5679.2018.00797; Piotr Pacek and Olaf Truszczyński, “Hybrid War and Its Psychological Consequences,” *Toruń International Studies* 1, no. 13 (2020): 23-30, https://doi.org/10.12775/TIS.2020.002.

[41] Yuriy Danyk et al., “The Technology of Objective Diagnosis, Treatment and Prevention of PTSD in Members of the Armed Forces under Conditions of Hybrid War,” *International Journal of Research and Innovation in Applied Science* 4, no. 1 (January 2019): 7-11, www.rsisinternational.org/journals/ijrias/DigitalLibrary/Vol.4&Issue1/07-11.pdf.

циальную агрессию против воображаемых угроз), вторжение травматических воспоминаний во все аспекты жизни и неверие в возможность избежать травматического опыта. Эту форму отличает от традиционной боевой травмы то, что вернувшиеся солдаты или участники боевых действий не возвращаются в состояние мира и стабильности, но по-прежнему живут в нестабильной среде, в которой угрозы и раздражители пронизывают повседневную жизнь.[42]

Стратегии гибридной войны не только многими путями создают непосредственные травматические ситуации, но и воспроизводят диссоциативные состояния так долго, что психобиологические реакции становятся неразличимыми. Описывая боевую травму, Кардинер писал: «…весь аппарат согласованной, скоординированной и целенаправленной деятельности разбит. Восприятие становится неточным и наполнено страхом, координационные функции суждения и различения не работают … органы чувств могут даже перестать функционировать».[43] В условиях гибридной войны человек, пытающийся преодолеть постоянный стресс и чувство угрозы, безнадёжности и потери контроля, не может вполне полагаться на более крупные социальные резервы устойчивости. Когда ощущается социальная травма и группы начинают распадаться, другие члены общества усиливают неуверенность и ощущение риска, и этот феномен существенно возрастает при доступе и использовании соцсетей.

Те, кто не участвовал в боевых действиях и не испытал насилия на фронте, тоже могут ощущать многие факторы стресса, связанные с посттравматическим стрессовым расстройством, и медицинские исследования показали, что длительное воздействие этих факторов сказывается на качестве биофизиологических маркеров.[44] Это, может быть, и не удивительно, учитывая методы гибридной войны, но любопытно, что киберинструменты позволяют острому стрессу проникнуть в районы географически удалённые от традиционных конфликтов. Эти синдромы возникают как следствие длительной коллективной и индивидуальной травмы от угроз жизни и здоровью, постоянного изменения форм и интенсивности боевого напряжения, продолжительности боевых действий и специфического небоевого стресса разной силы. Всё это часто превышает возможности психологической устойчивости человека. Традиционными факторами посттравматического стрес-

---

[42] Judith L. Herman, *Trauma and Recovery: The Aftermath of Violence – From Domestic Abuse to Political Terror* (New York: Basic Books, July 2015).

[43] Цитата из Herman, *Trauma and Recovery*, 35.

[44] Iryna Boichuk et al., "Characteristics of Eye Movements in the Anti-terrorist Operation Area's Residents with Potential Posttraumatic Stress Disorder," *Journal of Opthamology* 1 (Ukraine) (2019): 52-55; Yuriy Danyk et al., "The Objectivization of the Complex PTSD Diagnostic by Identifying Opthalmological Biomarkers," *International Journal of Research and Innovation in Applied Science* 4, no. 2 (January 2019): 7-11, www.rsisinternational.org/journals/ijrias/DigitalLibrary/Vol.4&Issue1/07-11.pdf.

сового расстройства являются потеря товарищей и участие в насилии в отношении врага. В гибридных кампаниях, наподобие украинской, эффект усиливается на фоне сложной этнонациональной идентичности. В то же время масштаб и географический охват внешних факторов стресса преднамеренно разрывает социальные ткани, лишая людей чёткого представления о том, где они находятся и во что им верить с точки зрения текущих событий и будущих целей. Под сомнение ставятся идеи мирной жизни, стандартные ценности общества, оценки участников боевых действий мирными гражданами.

В Украине гражданам приходится противостоять конкурирующим версиям о том, что конфликт в Донецкой и Луганской областях является результатом российского вторжения, гражданской войной между украинцами, следствием этнического разделения русских и украинцев, борьбой за свободу и независимость от коррумпированного украинского правительства или частью более масштабного экспансионистского проекта «Новороссии». Доминирующий нарратив отсутствует намеренно. Чем меньше согласия относительно природы конфликта, его причин и оценки его участников, тем больше напряжения и разногласий может возникнуть в мирных районах Украины и соседних странах. В отличие от усиления коллективной идентичности перед лицом явного агрессора (американский идеал Второй мировой войны), в гибридной войне никто не знает, кто на самом деле агрессор и почему. Мир может наступить в любое время или не наступить никогда, история становится туманной, а ощущение стабильности – эфемерным.[45]

Способность населения протестовать против конфликта или поддерживать его тоже можно использовать как средство эксплуатации гибридной войны в целевой стране. Разочарование и негодование, порождённые масштабным конфликтом, в сочетании с мыслями о коррупции или злоупотреблениях политической, военной и деловой верхушки могут легко усиливать различные киберкампании и целевое воздействие. Ухудшение социально-экономических условий и невозможность изменить жизнь к лучшему можно рефлекторно контролировать, чтобы изменить результаты выборов или вызвать миграцию из одного региона в другой. В этом случае мигранты могут стать мишенью, как участники этнического или культурного «вторжения» для изменения политических настроений в третьей стране. Это явление наблюдалось как в Украине по отношению к внутренне перемещенным лицам из Крыма/Донецка/Луганска, так и в недовольстве украинцами, переехавшими в такие страны, как Польша. Кампании дезинформации в российских СМИ сработали против сирийских беженцев в Германии и латиноамериканских мигрантов в Соединённых Штатах Америки при помощи лжи-

[45] Joanna Szostek, “Nothing Is True? The Credibility of News and Conflicting Narratives during ‘Information War’ in Ukraine,” *The International Journal of Press/Politics* 23, no. 1 (January 2018): 116-35, https://doi.org/10.1177/1940161217743258.

вых историй, которые вбрасывались и распространялись внутренними источниками в Германии и США.[46]

Угрозы кибербезопасности из-за пандемии COVID-19 в условиях гибридной войны и кибер-социальные уязвимости

Пандемия COVID-19 стала серьёзным испытанием эффективности систем здравоохранения во всем мире и способности государств, местных и национальных органов власти противостоять соответствующим вызовам и угрозам безопасности. Хотя понятное внимание к пандемии коронавируса попрежнему сосредоточено главным образом на прямом воздействии на здоровье населения и реагировании на экономические последствия, вспышка резко изменила взаимодействие в обществе с применением информационных технологий. Киберсистемы и информационные технологии могут предоставить некоторые полезные возможности, но необходимо также выявить и устранить системные риски и уязвимости безопасности в условиях гибридной войны.

Непосредственным последствием пандемии COVID-19 в Китае стала не только изоляция городов друг от друга и полная блокада города Ухань, но и введение обязательных приложений для отслеживания на личных телефонах. Южная Корея отправляла подробные описания перемещений людей, подозреваемых в заражении, что вызывает серьёзные опасения по поводу конфиденциальности и точности данных.[47] Такая политика отслеживания отражает технологические возможности контроля перемещений, помогая прогнозировать распространение таких инфекционных заболеваний, как коронавирус. Тем не менее они применялись, на фоне опасений по поводу внутренней безопасности, частной жизни и возможного использования правительственными и неправительственными организациями, особенно с учетом региональных и геополитических трансформаций, вызванных пандемией COVID-19.

Европейская комиссия в 2020 г. объявила о намерении отслеживать перемещение граждан с помощью мобильных технологий. Европейский комиссар по внутреннему рынку и услугам Тьери Бретон заверил, что план ЕС не ставит целью контролировать людей, данные останутся анонимными и будут удалены после пандемии. Европейский инспектор по защите данных заявил, что это решение не нарушает правил конфиденциальности. Vodafone, Deutsche Telekom, Orange, Telefonica, Telecom Italia, Telenor, Telia и A1 Telekom Austria согласились предоставить данные. В Германии такое

[46] Stefan Meister, “The ‘Lisa Case’: Germany as a Target of Russian Disinformation,” *NATO Review*, July 25, 2016, https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm; Howard et al., “The IRA, Social Media and Political Polarization.”

[47] Олег Мавеичев, «Что получил Китай за три последних месяца», *LiveJournal*, 20 марта 2020, https://matveychev-oleg.livejournal.com/9896483.html.

наблюдение запрещено законом. Тем не менее пандемия COVID-19 вызвала дискуссию о необходимости затронуть фундаментальные права граждан, особенно со стороны государства, которое уже вводит существенные ограничения на свободу передвижения. Министр здравоохранения Германии Йенс Шпан был первым, кто предложил собирать данные с мобильных телефонов инфицированных людей.[48]

Deutsche Telekom уже предоставил Институту Роберта Коха (RKI) информацию о миллионах своих клиентов. RKI специализируется на изучении инфекционных заболеваний и принимал активное участие в обсуждении информационной политики при пандемии COVID-19. Вирусологи RKI хотели составить карты перемещения жителей Германии и понять, как долго люди в городских условиях подвергались воздействию вируса во время карантина, вызванного пандемией. Эта информация позволила более точно предсказать распространение инфекционных заболеваний, а также разработать систему быстрого расчёта всех социальных связей данного человека: с кем он контактировал, с кем путешествовал, где был и с кем общался.[49] Например, подобные системы массового наблюдения внедрены в таких странах, как Китай и Россия. В России премьер-министр Михаил Мишустин предложил отслеживать всех подозреваемых в заражении COVID-19 по геолокации их мобильных телефонов. Многие страны также предлагали новые программы эпиднадзора для лучшего планирования потребностей больниц и имеющихся ресурсов, но это требует существенного смягчения конфиденциальности медицинских данных и создаёт дилемму между конфиденциальностью, общественным благом и доверием к учреждениям, хранящим такую информацию.[50]

Доверие, фейки и дезинформация

Вопрос доверия выходит за сферу деятельности отдельных правительств. В катастрофических ситуациях достоверная информация – всегда ценный ресурс, а в условиях длительного стресса люди более уязвимы к инсинуациям, слухам и намеренной дезинформации. Лёгкость распространения такой дезинформации по миру существенно повышают современные информационные сети, от мессенджеров до соцсетей. Пандемия COVID-19 создала благоприятную почву для появления и распространения теорий заговора. Когда информации недостаточно, а неопределённость высока, вакуум

[48] Foo Yun Chee, “Vodafone, Deutsche Telekom, 6 Other Telcos to Help EU Track Virus,” *Reuters*, Technology News, March 25, 2020, по состоянию на 1 апреля 2020, https://uk.reuters.com/article/us-health-coronavirus-telecoms-eu/vodafone-deutsche-telekom-6-other-telcos-to-help-eu-track-virus-idUKKBN21C36G.

[49] “Geolocation Surveillance: What Is Allowed in Germany for the Fight Against Coronavirus,” *DW Made for Minds Journal*, April 2020.

[50] Radu Mîrza, “COVID-19 and Digital Rights in Romania, Moldova and Ukraine,” *Central and Eastern European EDem and EGov Days* 341 (March 2022): 195-211, https://doi.org/10.24989/ocg.v341.14.

легко заполняет дезинформация и истории, которые невозможно проверить.[51] Коронавирус несёт особые проблемы, связанные с дезинформацией: долгий инкубационный период, возможность передачи бессимптомными носителями, зарубежное происхождение вируса в сочетании с дилеммой политики общественного здравоохранения, которая может оказаться отрицательной. Примерные прогнозы потенциальных смертей могут быть изменены из-за значительного социального дистанцирования, а первоначальные оценки – завышены. Экономические издержки более очевидны и непосредственны, в то время как выгоды для общественного здравоохранения в значительной степени эфемерны, пока они не исчезают.[52]

Одна из главных баек о коронавирусе заключалась в том, что он создан искусственно в лаборатории некой страны. Спор 2019 г. о китайском учёном из Национальной микробиологической лаборатории в Виннипеге послужил основой для измышлений о том, что правительство Канады создало вирус, который затем украл и распространил китайский учёный.[53] Спор Канады с китайской телекоммуникационной компанией Huawei тоже стал частью теории заговора, согласно которой вирус распространяют сети 5G. Заговор 5G, проявившийся в Великобритании, вылился в многочисленные нападения на вышки сотовой связи.[54] Во многих странах в 2020-2022 гг. циркулировала разнообразная информация о пандемии со значительными неточностями и ложными сведениями/ дезинформацией.[55] Эта часто противоречивая информация звучала на многих официальных брифингах и в новостях почти обо всех аспектах COVID-19.[56]

Противоречивые сообщения о реакции государства, информация и комментарии СМИ практически во всех странах создали серьёзную путаницу в отношении масштаба рисков пандемии, с резкими расхождениями по поводу опасности вируса. Звучали утверждения о том, что некоторые деятели используют средства массовой информации для сговора, чтобы подорвать

---

[51] Sally McManus, Joanna D'Ardenne, and Simon Wessely, "Covid Conspiracies: Misleading Evidence Can Be More Damaging Than no Evidence at All," *Psychological Medicine*, no. 1-2 (2020), https://doi.org/10.1017/S0033291720002184.

[52] Edward Lucas, "Mutations of Misinformation," *Tyzhden.ua*, March 1, 2020, по состоянию на 5 апреля 2020, https://tyzhden.ua/Columns/50/240946.

[53] Dax Gerts et al., "'Thought I'd Share First' and Other Conspiracy Theory Tweets from the COVID-19 Infodemic: Exploratory Study," *JMIR Public Health and Surveillance* 7, no. 4 (April 2021): e26527, https://doi.org/10.2196/26527.

[54] Takele T. Desta and Tewodros Mulugeta, "Living with COVID-19-Triggered Pseudoscience and Conspiracies," *International Journal of Public Health* 65, no. 6 (2020): 713-714, https://doi.org/10.1007/s00038-020-01412-4.

[55] Sahil Loomba et al., "Measuring the Impact of COVID-19 Vaccine Misinformation on Vaccination Intent in the UK and USA," *Nature Human Behaviour* 5, no. 3 (2021): 337-348, https://doi.org/10.1038/s41562-021-01056-1.

[56] Emily Chen et al., "COVID-19 Misinformation and the 2020 U.S. Presidential Election," *Harvard Kennedy School (HKS) Misinformation Review*, March 3, 2021, https://doi.org/10.37016/mr-2020-57.

авторитет определённых политиков или медицинских специалистов, и что утверждения о возможном заражении и смерти от COVID-19 сильно преувеличены. Такие схемы дезинформации в Украине не просто сеяли стресс и неуверенность. Можно вспомнить хотя бы яростные протесты в Украине, разразившиеся в феврале 2020 г. из-за ложной информации о рисках распространения вируса гражданами, возвращающимися из Китая. Дезинформация о пандемии распространялась в соцсетях в Украине в 2020-2021 гг. и серьёзно подрывала действия правительства.

Поэтому дезинформацию планируют так, чтобы множить неопределённость и сеять сомнения. Тексты и сообщения часто подаются в доверительной форме, с обращением к близкому другу. Обычно они содержат всю информацию о том, что может заинтересовать получателя, включая призыв к действию. Людям говорят, что делать, чтобы защитить себя; их также просят распространить эту «секретную» бесценную информацию, чтобы помочь как можно большему числу людей. Такие сообщения часто мотивируют тем, что власти якобы скрывают пути решения проблемы пандемии или её происхождение. Источник информации обычно не указывают, ссылаясь на эксперта или знакомого. Информация может исходить как от иностранцев, планирующих спровоцировать беспорядки, так и от сограждан, финансово заинтересованных в распространении дезинформации. В 2020 г. усилия КНР по дезинформации заметно сместились в сторону индивидуальных пользователей телефонных мессенджеров в США, в частности, для распространения дезинформации о COVID.[57]

Кампании дезинформации не только влекут долгосрочные последствия для отдельных лиц, которые могут творить зло, но и наносят ущерб социальной и политической структуре, когда невозможно отличить достоверную информацию от ложной. Информационные технологии децентрализации источников новостей делают быстрое распространение ложной информации практически неконтролируемым и труднопреодолимым. После чернобыльской катастрофы 1986 г. в Украине часто говорили, что сотни людей погибли от радиации, а тысячи – от информации. Во время пандемии трудно подсчитать число жертв неточной информации, лжи или дезинформации, но по самым скромным оценкам, тысячи жизней можно было бы спасти при более своевременном вмешательстве правительства и действиях системы здравоохранения.[58]

Столь сильное киберинформационное воздействие у многих вызывает

---

[57] Edward Wong, Matthew Rosenberg, and Julian E. Barnes, “Chinese Operatives Helped Sow Panic in U.S., Officials Say,” *The New York Times*, April 23, 2020, A10.

[58] Nicholas Charron, Victor Lapuente, and Andrés Rodriguez-Pose, “Uncooperative Society, Uncooperative Politics or Both? How Trust, Polarization and Populism Explain Excess Mortality for COVID-19 across European Regions,” The QoG Institute Working Paper 12 (Göteborg, Sweden: The Quality of Government Institute, Department of Political Science, University of Gothenburg, December 2020), http://hdl.handle.net/2077/67189.

стрессовое состояние, сохраняющееся длительное время с разной интенсивностью. Данное состояние можно охарактеризовать как «пандемический информационный стресс», который в дальнейшем может претерпеть различные психосоматические изменения: посттравматическое стрессовое расстройство (ПТСР), развитие тревожно-депрессивных состояний, приступы паники, формирование фобий и последствия обсессивно-компульсивных расстройств. На их появление и развитие существенно влияют состояние экономики, угроза снижения уровня жизни, безработица и неуверенность в будущем.[59] Глобальной тенденцией стало тиражирование ложной информации в социальных сетях, распространение фото и видео без понятного контекста, но с чёткой эмоциональной направленностью, достоверность которых сложно оценить при просмотре. Во время пандемии подобные информационные воздействия влекут особо тяжкие социальные последствия и становятся мощным инструментом гибридной войны.

Киберпреступность и шпионаж

Связанная, но отдельная проблема – рост киберпреступности. Некоторые преступления прямо связаны с медицинскими учреждениями и их информационными системами. Например, преступники ищут информацию о лекарствах, испытаниях или вакцинах от короновируса для продажи на чёрном рынке. Ещё одной тенденцией является оборот поддельных так называемых лекарств от коронавируса на открытом рынке, учитывая всеобщую осведомленность о вирусе и сильное желание избежать заражения. Кроме того, деструктивные кибердействия направлены на взлом лечебных учреждений и кражу конфиденциальных данных. Также были попытки шифровать большие объёмы важных медицинских данных для получения выкупа за их восстановление. Пандемия сделала больницы, научные центры и университеты беззащитными перед организованными киберпреступниками. Атакам подверглись университетская больница в Брно (Чехия) – крупный центр тестирования на COVID-19, британская компания Hammersmith Medicines Research, разрабатывающая вакцины от COVID-19, парижская больница AP-HP и ряд испанских больниц. Кроме того, Всемирная организация здравоохранения (ВОЗ) предупредила о подозрительных электронных письмах, полученных от злоумышленников, пытавшихся воспользоваться чрезвычайной ситуацией для кражи денег и конфиденциальной информации, а также о попытках взлома компьютерных систем ВОЗ и её базы данных по коронавирусу.[60] Президент Еврокомиссии Урсула фон дер Ляйен

[59] Ali Farooq, Samuli Laato, and AKM Najmul Islam, “Impact of Online Information on Self-Isolation Intention during the COVID-19 Pandemic: Cross-Sectional Study,” *Journal of Medical Internet Research* 22, no. 5 (2020): e19128, https://doi.org/10.2196/19128.

[60] World Health Organization, “Beware of Criminals Pretending to be WHO,” April 2020, по состоянию на 5 апреля 2020, https://www.who.int/about/cyber-security.

предупредила, что в ЕС выросла киберпреступность из-за вспышки коронавируса. «Они следят за нами в Интернете и используют наш страх коронавируса. Наш страх – это их бизнес-возможность», – пишет EU Observer.[61]

Внезапный переход к удаленной работе и банковскому обслуживанию также подвергает многих людей опасности воровства через финансовые системы или коммерческие и промышленные сети, никогда не предназначавшиеся для широкого распространения. Эксперты по кибербезопасности опасаются, что предприятия будут использовать упрощенные методы обеспечения сетевой безопасности, чтобы сохранить прибыль во время серьёзного экономического спада. Коммерческая и промышленная информация будет передаваться через частные сети и на персональные компьютеры, а служба информационной безопасности не сможет контролировать использование этих открытых сетей. В странах, которые до пандемии уже подвергались риску промышленного шпионажа, киберпреступники и посторонние лица обязательно увидят открывшиеся им возможности.[62]

Образование и переход к электронному обучению

Образование – ещё один важный вопрос, прямо связанный с пандемией и кибер-социальными уязвимостями в условиях гибридной войны. Из-за связанного с COVID карантина произошли глубокие изменения в установившемся ритме жизни, работы и обучения всех групп населения почти во всех странах. Человечество впервые столкнулось с пандемией такого уровня в условиях высокотехнологического информационного общества, глобализации и доступности поездок по всему миру. В одночасье были нарушены бизнес, туризм, миграция и мобильность населения. Вынужденный, реальный, быстрый и массовый переход к электронному обучению во всех сферах и на всех уровнях образования стал стрессом для всех участников образовательного процесса, которым пришлось в спешном порядке осваивать новые инструменты и методы.

Образование в условиях пандемии стало стратегической проблемой с далеко идущими последствиями для всего мира. Генеральный секретарь ООН Антониу Гутерреш отметил, что около миллиарда студентов и школьников в 160 странах мира не могли получить полноценное образование из-за закрытия учебных заведений, вызванного эпидемией коронавируса. Это грозит миру «катастрофой поколений». Согласно опросам, проведенным в Украине в июле 2020 г., и оценкам Госслужбы качества образования Украины, электронное обучение в школах не поддерживают 48 % родителей и

---

[61] "The EU Recorded a Sharp Increase of Cybercrime: What Is Happening," *Informacionnoe Soprotivlenie*, March 25, 2020, по состоянию на 1 апреля 2020, https://sprotyv.info/analitica/v-es-zafiksirovali-rezkij-rost-kiberprestupnosti-chto-proishodit.

[62] Eduard Babulak, James C. Hyatt, Kim Kyu Seok, and Jang Sun Ju, "COVID-19 & Cyber Security Challenges US, Canada & Korea," *Transactions on Machine Learning and Data Mining* 13, no. 1 (2020): 43-59, http://www.ibai-publishing.org/journal/issue_mldm/2020_October/13_2_43_59_mldm.pdf.

45 % учащихся, а «полностью поддерживают» электронное обучение лишь 9,9 % опрошенных.[63]

Проблемы заключаются не только в сути электронного обучения, но и в связанных с ним социотехнических противоречиях и киберсоциальных уязвимостях. Электронное обучение многогранно и междисциплинарно. Проблема включает технические, социальные, демографические, психологические, содержательно-информационные, методологические, дидактические, организационные, кибернетические и иные аспекты, а также способность правительств готовить кадры для планирования и проведения электронного обучения. Студенты должны уметь правильно и эффективно использовать технологии и беречь психическое и физическое здоровье в условиях неопределённости и стресса.

Проблемы образования, возникшие в условиях гибридного противостояния и пандемии, напрямую затрагивают все сферы функционирования государства и национальной безопасности. В целом это вопрос судьбы государства и государственности, их дальнейшего существования и развития. В отсутствие государственного контроля и регулирования электронное обучение потенциально может привести не только к усилению неравенства в образовании и потере человеческого потенциала, но и к опасным изменениям в обработке информации, критическом мышлении и зависимости от соцсетей. Это может сделать их уязвимыми для когнитивных и эмоциональных методов кибервойны.

Пандемия породила спрос на официальные стандарты электронного обучения специалистов и разработку курсов электронного обучения, которые помогут оценить эффективность электронного обучения и продвигать системный подход в новом режиме образования в разных странах, от США до Украины. Это означает, что электронное обучение требует стандартизации, систематизации и стратегических подходов для обеспечения эффективного дистанционного образования, одновременно предоставляя ресурсы для достижения целей на тактическом институциональном уровне. Пандемия рано или поздно закончится, но образование (гражданское, государственное и военное) вряд ли вернется к прежнему состоянию, и необходимо учитывать последствия этого для национальной безопасности. COVID-19 вызвал глубокие резкие изменения в обществе, и наша зависимость от технологий требует от государства разумных политических решений, касающихся не только реагирования на сам вирус, но и признания уязвимостей, создаваемых технологиями.

---

[63] Yuriy Danyk and Tamara Maliarchuk,“Strategic Aspects and Problems of E-learning in the Context of Pandemic and National Security,” *S-Direct 24* 3, no. 14 (July 2020), International scientific journal published under the auspices of NATO Defence Education Enhancement Program.

Заключение

Цель этой статьи – показать главные проблемы, созданные гибридной войной и COVID-19, и возможные пути их решения в киберпространстве, общественной жизни и национальной безопасности, охватывающие все сферы деятельности государства. Использование кибер-социальных уязвимостей играет важную и всё возрастающую роль в гибридных конфликтах. Создание эффективной национальной системы кибербезопасности и киберзащиты государства, включая характеристики кибер-социальных уязвимостей – один из главных приоритетов национальной безопасности и обороны. Эффективное заблаговременное предупреждение о кибер-социальных уязвимостях требует анализа структуры и параметров киберсистем и их пользователей и понимания того, как распространяются, принимаются и воспроизводятся сообщения в киберсистемах. Стратегии повышения устойчивости информационных систем опираются не только на модели «крепости» от злоумышленников, но и на готовность населения к уловкам, взломам и кампаниям дезинформации изнутри и извне.

Главной стратегической целью гибридной войны представляется дестабилизация – т.е. не физическая оккупация территории, а недоверие к институтам и самой информации. Такие атаки разрушают не только критическую инфраструктуру, но и общество. Установлено, что основные разрушительные кибердействия были выборочными и нацеленными на уязвимые киберсоциальные элементы. Разрушительные целенаправленные кибератаки проводились в рамках крупномасштабных комплексных кибероперациий.

Главные проблемы, возникшие или проявившиеся в связи с пандемией COVID-19 в контексте гибридной войны, таковы:

- Недостаточная готовность кибер-общественных систем здравоохранения большинства стран;
- Глубокая перестройка национальных экономик из-за реагирования на COVID-19 и формирования новых моделей жизни общества;
- Быстрое и полное погружение населения в киберпространство и переход к дистанционным (удалённым) формам работы и учёбы;
- Рост активности в соцсетях, увеличение объёмов онлайн-торговли, развлечений и услуг (дистанционная медицина, электронное обучение, электронное банковское обслуживание);
- Рост числа разнообразных киберпреступлений, распространение фейковых новостей, связанных с пандемией, дезинформация и информационное перенасыщение общества;
- Недостаточная киберинформационная грамотность, неумение или нежелание использовать интернет-системы и информационные технологии в повседневной жизни, а также неспособность обеспечить кибернетическую и информационную безопасность, особенно в условиях глобальной гибридной войны.

Хотя ранее мы уже говорили о развёртывании кибер-гибридных войн, пандемия COVID-19 усилила действия и уязвимости, связанные с конфиденциальностью, изоляцией, затруднением идентификации и распространением дезинформации.[64] Пандемия привела к усилению присутствия дестабилизирующих факторов в жизни людей, повышению зависимости от виртуальной информации, из-за разрыва традиционных социальных связей, а также росту зависимости от кибертехнологий во всех областях жизнедеятельности.

Особого внимания заслуживает введение контроля за соблюдением требований карантина с применением высоких технологий. Непринятие своевременных мер предосторожности для защиты прав граждан может привести к посягательству на конфиденциальность личной информации. Есть основания ожидать, что такой контроль и надзор за гражданами и их деятельностью во многих странах, особенно с авторитарными режимами, может не только сохраниться, но и усилиться после того, как утихнет пандемия. Такое развитие событий представляет угрозу для собственной страны и даёт возможность внешним игрокам использовать такие системы «социального кредита» в своих интересах. Чем больше мы зависим от таких технологий, тем больше уязвимостей позволяют использовать такие связи, сейчас в основном независимые от традиционной социальной устойчивости. Каковы последствия для безопасности, если посторонние меняют медицинские записи, вносят людей в списки не допущенных к полётам или подделывают их личность не только для подачи заявки на получение кредита, но и в мировых средствах массовой информации?

Пандемия COVID-19 потрясла мировую систему не только с точки зрения экономической активности и поездок за рубеж, но и в том, как мы относимся к технологиям, измеряем и ценим социальную и политическую стабильность, а также наши способности реагировать на спектр атак гибридной войны с использованием кибертехнологий и уязвимостей. Наши общества становятся всё более уязвимыми для когнитивной и эмоциональной войны, которая подавляет обработку нами информации, обходит рациональное мышление и поражает нас на базовом уровне «выживания», часто – в рамках стратегии, направленной на дальнейшее разделение наших обществ и недоверие к институтам. Хотя мы давно ожидали роста значимости кибергибридной войны, сейчас нужно устранить недостатки в дезинформации, конфиденциальности, киберпреступности и электронном обучении, которые могут повлиять на более важные вопросы безопасности и стабильности.

Таким образом, данное исследование помогает дать определение кибервойны или киберконфликта в киберпространстве. Противостояние в ки-

[64] Tamara Maliarchuk, Yuriy Danyk, and Chad Briggs, “Hybrid Warfare and Cyber Effects in Energy Infrastructure,” *Connections: The Quarterly Journal* 18, no. 1-2 (2019): 93-110, https://doi.org/10.11610/Connections.18.1-2.06.

берпространстве и (или) при помощи киберпространства – это сложное социально-политическое явление с использованием киберразведки, киберзащиты и кибероружия для нанесения противнику различных потерь в разных областях и минимизации собственных потерь в экономической, военной, политической, социальной, кибернетической, информационной, идеологической и других сферах. В отличие от других деструктивных действий, конфликтов и (или) войн, кибервойну (киберконфликт, деструктивные кибердействия) не объявляют. И если она началась, она не закончится, но будет продолжаться непрерывно до тех пор, пока одна из сторон конфликта не будет полностью разгромлена либо не сможет продолжать разрушительные действия. Она может завершиться только с уничтожением киберпространства.

Хотя военные стратегии по-прежнему действуют, удар всё чаще наносят «под дых» обществу.

Примечание

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

Благодарность

Connections: The Quarterly Journal, Vol. 20, 2021, вышел при поддержке правительства США.

Об авторах

Д-р **Чэд Бриггс** – доцент, руководитель кафедры государственной политики и управления Университета Аляски в Анкоридже. Д-р Бриггс имеет опыт информационной и гибридной войны, а также разработки оборонительных стратегий защиты критически важных систем в Восточной Европе и на Балканах. Имеет степень доктора политологии Карлтонского университета в Канаде. Ранее был старшим советником Министерства энергетики США, зав. кафедрой «Минерва» и профессором энергетической и экологической безопасности Авиационного университета ВВС США. Соавтор (совместно с Мириам Матеёвой) труда *Disaster Security: Using Intelligence and Military Planning for Energy and Environmental Risks*.
Электронная почта: chad.briggs@alaska.edu

Генерал-майор **Юрий Даныk**, профессор, доктор технических наук, Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского». Д-р Даник является экспертом в области военного искусства, национальной обороны и безопасности, информационной и кибербезопасности, электронных и информационных технологий, разработки и применения робототехнических комплексов, а также развития сил специального назначения. Имеет боевой опыт применения передовых оборонных технологий в условиях современной войны.
Электронная почта: zhvinau@ukr.net

Д-р **Тамара Малярчук** была членом рабочей группы НАТО по реализации программы DEEP в Вооружённых силах Украины. Была аналитиком Житомирского военного института им. С. Королева (Украина) и сотрудничала с ВС США по вопросам языковой и кибернетической защиты. Занимается исследованиями в области электронного обучения, инновационных технологий обнаружения и терапии посттравматического стрессового расстройства, а также манипулятивных сетевых технологий.
Электронная почта: maliarchuktamara@gmail.com