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

Хезер Грегг, *Connections QJ* 23, № 2 (2024): 169-182
https://doi.org/10.11610/Connections.rus.23.2.01

Рецензированная статья

Гибридные угрозы и стратегическое соперничество

Хезер Грегг

Европейский центр исследований в области безопасности им. Джорджа Маршалла, https://www.marshallcenter.org

Аннотация: Стратегическое соперничество не является чем-то новым, как и меры правительств по формированию международной системы в своих интересах, не прибегая к войне. Однако способность государственных и негосударственных субъектов напрямую влиять на население посредством быстрых и скрытых действий отличается от предыдущих проявлений стратегического соперничества. Такие действия, которые мы в этой статье называем гибридными угрозами, прямо угрожают суверенитету государств и являются главной негативной чертой современного стратегического соперничества. В статье мы поясним это, дав рабочие определения стратегического соперничества и его отличия от соперничества великих держав; объяснив, что такое гибридные угрозы и гибридная война и какова их роль в более широких стратегических целях государственных и негосударственных субъектов; показав, как стратегические соперники и противники воспринимают эти действия; и отметив важность формирования стойкости населения к гибридным угрозам.

Ключевые слова: гибридные угрозы, гибридная война, нерегулярная война, стратегическое соперничество, соперничество великих держав, неограниченная война, политическая война, действия в серой зоне.

Вступление

Стратегическое соперничество не ново, как и меры правительств по формированию международной системы в своих интересах, не прибегая к войне. Например, в XIX веке Британская и Российская империи предпринимали экономические, политические, дипломатические и разведывательные меры в Центральной Азии, борясь за влияние и контроль в так называемой

«Большой игре». Во время Холодной войны США и их союзники тоже противодействовали СССР посредством внешнеполитических хитросплетений, не предполагающих полномасштабной войны, чтобы сформировать международную систему в своих интересах и избежать эскалации до обычной и ядерной войны. Эти действия, по сути, являются основой международных отношений.

Возвращение к «соперничеству великих держав» после незаконной аннексии Крыма Россией в 2014 году и угроз Китая морским путям в Южно-Китайском море вновь привлекло внимание к действиям, не предполагающим открытой войны, для формирования международной системы. Хотя этот этап стратегического соперничества имеет некоторое сходство с его историческими предшественниками, его делает уникальным ряд факторов, включая новые технологии и усиление негосударственных игроков с глобальным влиянием и сферой деятельности. Возможно, главное отличие этого этапа стратегического соперничества от более ранних состоит в способности напрямую влиять на население другого государства посредством действий, влияющих на способность этого государства использовать силу внутри страны и за рубежом. Эти действия, называемые в нашей статье «гибридными угрозами», прямо угрожают суверенитету государств и являются определяющей чертой современного стратегического соперничества.

Страны Запада сталкиваются с рядом проблем, реагируя на гибридные угрозы со стороны противников, стремящихся повлиять на их население. Наиболее значимой из этих проблем является отсутствие консенсуса в терминологии, что затрудняет совместное противодействие гибридным угрозам на новом этапе стратегического соперничества. Чтобы решить эту проблему, в статье даётся чёткое определение терминов для описания субъектов, их целей и тактики формирования существующей международной системы и влияния на неё. В частности, различается соперничество великих держав и стратегическое соперничество, дано определение и классификация типов гибридных угроз, используемых при стратегическом соперничестве, и их целей, отличие гибридных угроз от гибридной войны, и содержится вывод о том, что эффективные контрмеры должны предусматривать формирование государствами стойкости своего населения.

Отличие соперничества великих держав от стратегического соперничества

Возможно, одной из главных проблем для понимания гибридных угроз как элемента стратегического соперничества является отсутствие консенсуса в том, что такое стратегическое соперничество и чем оно отличается, если вообще отличается, от соперничества великих держав. Хотя эти термины часто используют как взаимозаменяемые, это не синонимы. В США начали использовать термин «соперничество великих держав», чтобы сместить приоритеты безопасности с «глобальной войны с терроризмом» на устранение

угроз, исходящих от «примерно равных государств-соперников», после незаконной аннексии Крыма Россией в 2014 году.[1] В Стратегии национальной обороны 2015 года, принятой администрацией Обамы, соперничество великих держав было обозначено как ключевая проблема, и этот акцент сохранился в документах по национальной безопасности администраций Трампа и Байдена.[2] В этих и других документах подчёркивается угроза со стороны России и Китая.

В соперничестве великих держав участвуют примерно равные противники, использующие ряд инструментов государственного управления, угрожающих международному порядку. Решающее значение в соперничестве великих держав имеет способность и возможность государства создавать и применять силу при помощи своего военного, ядерного арсенала, экономической мощи, дипломатического влияния и умения привлекать других участников международной системы и влиять на них. Кроме того, требуется мудрость эффективно сочетать эти элементы для стратегического успеха. Эти возможности соответствуют тому, что Джозеф Най классифицировал как жесткую, мягкую и умную силу, соответственно.[3]

Стратегическое соперничество отличается от соперничества великих держав рядом ключевых аспектов. В частности, в стратегическом соперничестве участвуют не только «примерно равные соперники», такие, как Китай и Россия. В нынешней международной системе различные государственные и негосударственные игроки бросают вызов мировому политическому, экономическому и военному статус-кво – так называемому «порядку, основанному на правилах» – чтобы перестроить систему в своих интересах. Создание БРИКС в 2010 году (в составе Бразилии, России, Индии, Китая и ЮАР) и включение в него ещё пяти стран в 2024 году (Египет, Эфиопия, Иран, ОАЭ и Саудовская Аравия) стало серьёзным вызовом для возглавляемых Западом глобальных финансово-экономических институтов, созданных после Второй мировой войны.[4] Появление новых союзов в сфере безопасности,

---

1 Jim Garamone, “Dempsey: U.S. Forces Must Adapt to Deal with Near-Peer Competitors,” *Joint Chiefs of Staff*, August 17, 2015, по состоянию на 22 января 2024, www.jcs.mil/Media/News/News-Display/Article/613868/dempsey-us-forces-must-adapt-to-deal-with-near-peer-competitors/.

2 Ronald O’Rourke, “Great Power Competition: Implications for Defense – Issues for Congress,” *Congressional Research Services*, October 3, 2023, Report R43838, по состоянию на 22 января 2024, https://sgp.fas.org/crs/natsec/R43838.pdf; См. еще Michael J. Mazarr, Bryan Frederick, and Yvonne K. Crane, *Understanding a New Era of Strategic Competition* (Santa Monica: RAND, November 2022), www.rand.org/pubs/research_reports/RRA290-4.html.

3 Joseph S. Nye, Jr., *Soft Power: The Means to Success in World Politics* (New York: Public Affairs Books, 2005).

4 Alyssa Ayres, “How the BRICS Got Here,” *Council on Foreign Relations*, August 31, 2017, по состоянию на 22 января 2024, https://www.cfr.org/expert-brief/how-brics-got-here.

особенно с поставками оружия, тоже представляет собой вызов существующему международному порядку. Например, член НАТО Турция поддерживает связи с рядом стран, оспаривающим западные правила и нормы, включая Россию. В 2023 году Турция стала одним из ведущих производителей вооружений, в частности, БПЛА Akinci, которые она теперь экспортирует в разные страны, включая Саудовскую Аравию и Пакистан.[5]

Государства с региональными амбициями оказывают влияние, меняя стратегическую картину. Так, Катар взял на себя более активную дипломатическую роль на всём Ближнем Востоке, выступив посредником в переговорах США с Талибаном в Афганистане и в попытках добиться перемирия между ХАМАС и Израилем после нападения 7 октября 2023 года.[6] Важная роль Индии в создании БРИКС, а также её рост в качестве крупного потребительского рынка и экспортёра позиционируют её как серьезного игрока в региональной динамике и мировой экономике.[7] Как мы уже говорили, Турция тоже расширяет свое региональное и даже мировое влияние, экспортируя оружие.

На фоне этих вызовов нынешнему международному порядку негосударственные игроки продолжают участвовать в стратегическом соперничестве, как сами по себе, так и в качестве «прокси» государств, пытающихся бросить вызов мировому порядку. Например, ХАМАС спровоцировал изменение военной политики и приоритетов помощи США, напав на Израиль 7 октября 2023 года. Степень самостоятельности действий ХАМАС или их сотрудничества с Ираном и другими государствами остается предметом дискуссий.[8] Не менее важно, что несмотря на поражение Исламского государства в Сирии и Ираке, ИГИЛ остаётся главным приоритетом безопасности в ряде регионов, особенно в странах Субэкваториальной Африки, где ИГИЛ и Аль-Каида угрожают стабильности, побуждая вмешиваться страны Запада, Россию и Китай.[9]

В целом, в стратегическое соперничество вовлечён целый ряд государственных и негосударственных игроков, оспаривающим разработанные на

---

[5] Ali Bakir, “Turkey’s Defense Industry Is on the Rise: The GCC Is One of Its Top Buyers,” *Atlantic Council*, August 4, 2023, https://www.atlanticcouncil.org/blogs/menasource/turkey-defense-baykar-gcc-gulf/.

[6] Stephen Kalin, “Gaza Diplomacy Cements Qatar’s Global Mediator Role,” *The Wall Street Journal,* November 25, 2023, по состоянию на 27 января 2024, www.wsj.com/world/middle-east/gaza-diplomacy-cements-qatars-global-mediator-role-29e0ffb7.

[7] Bhaskar Chakravorti and Gaurav Dalmia, “Is India the World’s Next Great Economic Power?” *Harvard Business Review*, September 6, 2023, по состоянию на 2 февраля 2024, https://hbr.org/2023/09/is-india-the-worlds-next-great-economic-power.

[8] Fatima Al-Kassab, “What Is the ‘Axis of Resistance’ of Iran-Backed Groups in the Middle East?” *NPR*, October 26, 2023, по состоянию на 22 января 2024, www.npr.org/2023/10/26/1208456496/iran-hamas-axis-of-resistance-hezbollah-israel.

[9] Jason Warner et al., *The Islamic State in Africa: The Emergence, Evolution, and Future of the Next Jihadist Battlefront* (New York: Oxford University Press, 2021), https://doi.org/10.1093/oso/9780197639320.001.0001.

Западе экономические, правовые, политические нормы и институты безопасности.[10] Россия и Китай могут представлять главную угрозу, но бросить вызов мировой системе способны не только они.

Гибридные угрозы, гибридная война и стратегическое соперничество

Эпоха стратегического соперничества связана со способностью и готовностью государственных и негосударственных игроков формировать региональную динамику и международную систему в своих интересах. Но стратегическое соперничество сегодня отличает способность этих игроков напрямую воздействовать на население страны, чтобы помешать правительству использовать силу внутри страны и за рубежом. Эти действия, которые часто трудно обнаружить и ещё труднее приписать конкретному субъекту, мы называем гибридными угрозами. Фактически, сегодня гибридные угрозы могут быть основным инструментом стратегического соперничества.

Противодействие гибридным угрозам осложняет отсутствие консенсуса по терминам и общим целям таких действий в рамках стратегического соперничества. В Европе одно из наиболее широко принятых определений гибридных угроз дал Центр передового опыта по гибридным технологиям (Hybrid CoE), созданный в 2017 году по общей инициативе НАТО, ЕС и стран-партнёров. Центр был создан в ответ на незаконную аннексию Крыма и части восточной Украины Россией. Понятия гибридных угроз Hybrid CoE

> … означает действия государственных или негосударственных субъектов с целью ослабить или нанести ущерб объекту, влияя на принятие им решений на местном, региональном, государственном или организационном уровне. Такие действия координируются, синхронизируются и используют слабости демократических государств и институтов. Действия могут происходить, в частности, в политической, экономической, военной, гражданской или информационной сферах. Их проводят с использованием широкого арсенала средств и планируют так, чтобы не превысить порог выявления и установления виновных.[11]

В этом определении выделен ряд ключевых моментов для понимания гибридных угроз в контексте стратегического соперничества. Во-первых,

---

[10] Здесь имеются в виду институты согласно определению Дугласа Норта: «Институты — это созданные человеком ограничения, структурирующие политическое, экономическое и социальное взаимодействие. Они включают как неформальные ограничения (санкции, табу, обычаи, традиции кодексы поведения), так и формальные правила (конституции, законы, права собственности) … [чтобы] снизить неопределенность при взаимодействии». Douglas C. North, “Institutions,” *Journal of Economic Perspectives* 5, no. 1 (Winter 1991): 97-112, https://doi.org/10.1257/jep.5.1.97.

[11] Hybrid CoE, “Hybrid Threat as a Concept,” по состоянию на 22 января 2024, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

«концепция» Hybrid CoE называет источниками гибридных угроз как государственных, так и негосударственных игроков, указывая на то, что это не исключительно государственная деятельность. Например, в период своего подъёма ИГИЛ и Аль-Каида использовали разные тактики гибридных угроз, чтобы подорвать политическую легитимность и бросить вызов безопасности государств Ближнего Востока, Африки, Юго-Восточной Азии и Запада. Исследователь терроризма Брюс Хоффман отмечает, что теракты 11 сентября заставили США и их союзников полностью переориентировать свою внешнюю политику, изменив ход истории.[12]

Важно, что ИГИЛ и Аль-Каида поддерживали мощный потенциал информационной войны для пропаганды их грандиозных стратегических идей создания мировоззрения и политической системы, альтернативных западному светскому либерализму.[13] До распада Исламского государства в 2017 году ИГИЛ мог привлечь около 40 тыс. «иностранных боевиков» и сторонников в свой так называемый халифат в Сирии и Ираке.[14] Эти группировки по-прежнему способны совершать теракты по всему миру, используя грубую незаконную силу для влияния на действия государств. Поэтому можно сказать, что ИГИЛ и Аль-Каида по-своему стратегически соперничали с Западом. В Стратегии национальной обороны США 2018 года «экстремистские организации» фактически упомянуты наряду с четырьмя странами – Китаем, Россией, Ираном и Северной Кореей – как серьёзная угроза для США.[15]

Несмотря на отход от глобальной войны с терроризмом, негосударственные игроки продолжают играть заметную роль в стратегическом соперничестве как самостоятельно, так и в качестве так называемых «прокси», получающих государственную поддержку или финансирование. Как мы уже говорили, действия ХАМАС вынудили США и другие страны Запада пересмотреть свои приоритеты безопасности после нападения на Израиль 7 октября 2023 года. Таким образом, негосударственные игроки могут участвовать в стратегическом соперничестве, подрывая международный порядок и влияя на приоритеты внешней политики тех или иных стран.

---

[12] Bruce Hoffman, “Rethinking Terrorism and Counterterrorism Since 9/11,” *Studies in Conflict & Terrorism* 25, no. 5 (2002): 303-316, https://doi.org/10.1080/105761002901223.

[13] Samantha Mahood and Halim Rane, “Islamist Narratives in ISIS Recruitment Propaganda,” *The Journal of International Communication* 23, no. 1 (2017): 15-35, https://doi.org/10.1080/13216597.2016.1263231.

[14] Richard Barrett, “Beyond the Caliphate: Foreign Fighters and the Threat of Returnees” (New York, NY: The Soufan Center, October 2017), https://thesoufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf.

[15] U.S. Department of Defense, “ Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military’s Competitive Edge,” https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Во-вторых, определение Hybrid CoE ценно своим акцентом на последствиях гибридных угроз. Согласно их концепции, гибридные угрозы направлены на «намеренное воздействие на уязвимости демократических государств и институтов». Иными словами, гибридные угрозы направлены на использование различных уязвимостей внутри государства с конечной целью подрыва демократической системы страны. Эти уязвимости могут включать, в частности, этнические и/или религиозные различия населения, проблемы миграции, экономическое неравенство и разногласия по поводу ценностей и норм страны. В конечном счете, государственные и негосударственные игроки «используют» эти уязвимости как оружие для дальнейшего разделения и ослабления наций.

Например, в США исследователи и правоохранительные органы раскрыли попытки России использовать расовую напряжённость перед президентскими выборами 2016 и 2020 годов, включая активизацию в соцсетях со всех сторон расовых споров.[16] Важно отметить, что согласно Никласу Нильсену с коллегами, государственные и негосударственные субъекты могут действовать и против недемократических государств, что расширяет определение целей гибридных угроз на любые политические системы. Они утверждают, что эти игроки используют гибридные угрозы для «достижения результата без войны, чтобы нарушить, подорвать или ослабить политическую систему и сплоченность объекта…».[17] Этот более широкий взгляд помогает расширить обсуждение воздействия гибридных угроз при стратегическом соперничестве, поскольку он охватывает как государственные, так и негосударственные субъекты, участвующие в гибридных угрозах для дестабилизации и недемократических, и демократических государств.

Однако определение Hybrid CoE не отражает более широкую цель субъектов, использующих гибридные угрозы при стратегическом соперничестве: ослабление существующей мировой системы и её изменение в своих интересах. Как мы детально рассмотрим ниже, субъекты, прибегающие к гибридным угрозам, часто стремятся использовать существующие уязвимости внутри страны, чтобы ослабить и разделить её, тем самым не давая ей применить силу на региональном и глобальном уровнях. В этом контексте цель гибридных угроз заключается не просто в подрыве демократических институтов (или любой политической системы), но в разрушении этих институтов с тем, чтобы ослабить способность страны применить силу, тем самым позволяя государству действовать беспрепятственно и в конечном

[16] Jason Parham, “Targeting Black Americans, Russia’s IRA Exploited Racial Wounds,” *Wired*, December 17, 2018, по состоянию на 19 января 2024, www.wired.com/story/russia-ira-target-black-americans/.

[17] Niklas Nilsson et al., “Security Challenges in the Grey Zone: Hybrid Threats and Hybrid Warfare,” в *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations*, ed. Mikael Weissmann et al. (London: I.B. Tauris, 2021), 2, https://doi.org/10.5040/9781788317795.0005.

итоге изменять региональную или международную систему в своих интересах.

В-третьих, в определении Hybrid CoE подчёркивается, что гибридные угрозы включают «широкий арсенал средств и планируются так, чтобы не превысить порог выявления и установления виновных». Как правило, определения гибридных угроз основаны на ограниченном наборе действий, включая дезинформацию, вредоносную информацию и кибероперации типа атак DDoS или программ-вымогателей.[18] Однако определение Hybrid COE ценно тем, что оно допускает возможность «подтянуть» к гибридным угрозам практически всё. Марк Галеотти подробно исследует возможность использования в качестве оружия чего угодно – информации, ресурсов, преступных сетей и даже воображения – для воздействия на население и ослабления способности государства применить силу, особенно в эпоху возросшей взаимозависимости.[19]

Микаэль Вайссманн тоже рассматривает классификацию гибридных угроз, а не конкретные события. Его семь категорий включают дипломатическое,[20] экономическое, техническое, информационное, «нетрадиционное» (широкая категория, включающая такие виды деятельности, как терроризм и организованная преступность), гражданское (воздействие на гражданское общество) и некинетическое давление на военных, включая такие действия, как информационная война, призванная подорвать моральный дух войск противника.[21] Этот список категорий ценен, поскольку в нём описан ряд конкретных видов деятельности для контроля и будущего учёта. Например, много внимания уделено тому, как государственные и не-

[18] Дезинформация – это ложная информация, преднамеренно распространяемая с целью причинения ущерба. Вредоносная информация – это правдивая информация, преднамеренно распространяемая с целью причинения ущерба, а введение в заблуждение – это ложная информация, распространяемая без намерения причинения ущерба. Информация как гибридная угроза предполагает намерение, поэтому дезинформация и вредоносная информация – более подходящие термины. См. Claire Wardle, “Understanding Information Disorder,” *First Draft News*, September 22, 2020, по состоянию на 22 января 2024, https://firstdraftnews.org/long-form-article/understanding-information-disorder/.

[19] Mark Galeotti, *The Weaponization of Everything: A Field Guide to the New Way of War* (New Haven: Yale University Press, 2022).

[20] Хотя Вайссманн не уточняет этого, «публичная дипломатия» — это прямое обращение глав государств к населению, чтобы повлиять на него, что соответствует определению гибридной угрозы в этой статье, как направленной непосредственно на население. См. Mikael Weissmann, “Conceptualizing and Countering Hybrid Threats and Hybrid Warfare: The Role of the Military in the Grey Zone,” in *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations*, 65-66, https://doi.org/10.5040/9781788317795.0011.

[21] Weissmann, “Conceptualizing and Countering Hybrid Threats and Hybrid Warfare,” 65-66.

государственные субъекты используют в стратегических целях кибердействия, часто скрывая их.[22] Эти действия можно отнести к «технической» категории, по Вайссманну. Однако кроме кибердействий, техническая категория может включать быстро расширяющееся применение ИИ в качестве гибридной угрозы или потенциальное использование больших данных в стратегических целях. Таким образом, категории Вайссманна облегчают классификацию существующих действий и учитывают будущие возможности.

Кроме того, список гибридных угроз Вайссманна могли бы улучшить ещё две категории. Первая касается «ресурсов» как гибридной угрозы, в том числе энергии, продовольствия и воды, поскольку государственные и негосударственные субъекты используют эти уязвимости в стратегических целях. После полномасштабного вторжения России в Украину в 2022 году зависимость Европы от российской нефти и газа стала серьезной проблемой, что побудило ряд европейских стран снизить свою зависимость от российских энергоносителей.[23] Экспорт зерна из России и Украины тоже стал критической проблемой, которую можно использовать как оружие.[24] Вторая категория включает использование в качестве гибридных угроз культуры, ценностей и истории. В своём выступлении в сентябре 2022 года Владимир Путин заявил, что «диктатура западных элит направлена против всех обществ, в том числе и народов самих западных стран. Это вызов всем, такое полное отрицание человека, ниспровержение веры и традиционных ценностей». Он также представил свои действия в Украине и за её пределами как защиту исторических прав русских.[25] Поэтому культура, ценности и история представляют собой ещё один важный вид гибридных угроз.

Наконец, акцент Hybrid CoE на проблемах обнаружения гибридных угроз и, при обнаружении, установлении их источника имеет решающее значение для понимания этих действий в контексте стратегического соперничества. В весьма информативной книге Микаэля Вайссманна о гибридной войне отмечается, что «обман и отрицание присущи гибридным методам, и иногда трудно знать наверняка, что идёт война, и так же изначально трудно опре-

---

[22] Christian Payne and Lorraine Finlay, “Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack,” *The George Washington International Law Review* 49, no. 3 (2017): 535-568, https://149801758.v2.pressablecdn.com/wp-content/uploads/_pda/ILR-Vol-49.3_Panye-Finlay.pdf.

[23] Mark Finley and Anna B. Mikulska, “Wielding the Energy Weapon: Differences Between Oil and Natural Gas” (Houston: Rice University’s Baker Institute for Public Policy, June 26, 2023), https://doi.org/10.25613/G9P2-3F78.

[24] Josep Borrell, “Russia Must Stop Using Food as a Weapon,” *European Union External Action*, August 2, 2023, по состоянию на 27 января 2024, www.eeas.europa.eu/eeas/russia-must-stop-using-food-weapon_en.

[25] «Подписание договоров о принятии ДНР, ЛНР, Запорожской и Херсонской областей в состав России», 30 сентября 2022 года, http://www.kremlin.ru/events/president/news/69465 по состоянию на 22 января

делить, становится ли предполагаемая угроза будущих действий реальностью, и когда именно».[26] Концепция «околопороговой войны» Дэвида Килкаллена определяет несколько уровней атаки на основе атрибуции: от тайной (необнаруженное действие) до скрытой (обнаруженное действие неустановленного авторства), от двусмысленной (обнаруженное действие с подозреваемым, но не доказанным субъектом) до открытой (и действие, и субъект очевидны). Разрывы между этими типами атак усложняют задачу выработки своевременного пропорционального ответа без непреднамеренной или случайной эскалации конфликта. Килкаллен называет это «пороговой зоной» – это понятие тесно перекликается с серой зоной.[27]

Помимо определения гибридной угрозы Hybrid CoE, есть ряд дополнительных моментов, которые нужно учитывать. Во-первых, важно признать, что стратегическое соперничество не всегда означает применение государственными и негосударственными субъектами гибридных угроз против населения. Экономическая конкуренция, договора, союзы – это законные действия и часть «нормальных» международных отношений. Так, возникновение БРИКС в противовес западным финансово-экономическим институтам является примером законного и прозрачного стратегического соперничества. Напротив, гибридная угроза опирается на незаконные или юридически сомнительные («серые») действия, которые трудно отследить, нацеленные на население страны и в конечном итоге ослабляющие и ограничивающие способность государства применить силу.

Во-вторых, существуют разногласия по поводу использования термина «гибридная угроза» для описания этих действий. Американский дипломат Джордж Кеннан, участвовавший в разработке американской стратегии сдерживания СССР после Второй мировой войны, назвал такие действия «политической войной» – этот термин используют и сегодня.[28] С другой стороны, в Министерстве обороны США принят термин «нерегулярная война» для действий, схожих с гибридными угрозами. Совместная доктрина США, издание 1, том 1 «Совместные боевые действия», а также приложение о нерегулярной войне 2020 года к Стратегии национальной обороны определяют нерегулярную войну как «борьбу между государственными и негосударственными субъектами за влияние на население и легитимность». В определении далее поясняется, что «в нерегулярной войне предпочтение

---

[26] Weissmann, “Conceptualizing and Countering Hybrid Threats and Hybrid Warfare,” 63.

[27] David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, March 2020).

[28] О Кеннане см. “269. Policy Planning Staff Memorandum,” *Office of the Historian*, May 4, 1948, по состоянию на 21 января 2024, https://history.state.gov/historicaldocuments/frus1945-50Intel/d269. Пример использования термина «политическая война» сегодня: Linda Robinson et al., “The Growing Need to Focus on Modern Political Warfare,” Research Brief RB-10071-A (Santa Monica: RAND Corporation, 2019), https://www.rand.org/pubs/research_briefs/RB10071.html.

отдаётся непрямым военным действиям и асимметричным военным подходам, хотя может применяться весь спектр военных и иных возможностей для подрыва власти, влияния и воли противника». По сути, нерегулярная война описывает действия и цели, аналогичные гибридным угрозам.[29]

В дополнение к разным определениям на Западе, Китай и Россия разработали собственную терминологию для гибридных угроз. В 1999 году два китайских теоретика, Цяо Лян и Ван Сянсуй, ввели понятие «неограниченной войны». Они описали «будущее поле боя «расширенно», не поле боя, где прежде всего убивают, а поле боя, на котором цель любого национального государства (или субгосударственных субъектов) – «парализовать и дезорганизовать противника», прежде всего ослабив волю его народа и государства вести вооруженный конфликт».[30] Российский теоретик, начальник Генерального штаба Вооруженных сил страны генерал Валерий Герасимов также использовал термин «война без ограничений», чтобы описать использование Россией полного спектра операций по формированию региональной и международной системы в интересах России.[31]

Наконец, ряд учёных выступает за чёткое разграничение гибридных угроз и гибридной войны. Вайссманн, например, применяет определение гибридной войны Международного института стратегических исследований, чтобы отличить её от гибридных угроз:

> Использование военных и невоенных средств в комплексной кампании для достижения внезапности, захвата инициативы и получения психологических и физических преимуществ с использованием дипломатических средств; сложные и быстрые информационные, электронные и кибероперации; скрытые, а иногда и открытые военные и разведывательные действия; и экономическое давление.[32]

Важно различать гибридные угрозы и гибридную войну в контексте стратегического соперничества. Использование военных «инструментов» – от «некинетических» действий, таких, как размещение войск, до реального применения силы – обычно заметно и говорит о намерениях одного государства другому. Гибридные же угрозы менее очевидны, что усложняет их обнаружение и своевременный действенный ответ. Кроме того, гибридная война подразумевает прямое воздействие на население и вооружённые

---

[29] Сейчас МО США работает над новым определением нерегулярной войны.

[30] Согласно Марку Томасу. См. Mark Thomas, “The Chinese Roots of Hybrid Warfare,” *CEPA*, August 10, 2022, по состоянию на 20 января 2024, https://cepa.org/article/the-chinese-roots-of-hybrid-warfare/.

[31] Thomas, “The Chinese Roots of Hybrid Warfare.” См. также: ARIS, *“Little Green Men”: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014* (Fort Bragg, NC: The United States Army Special Operations Command, 2018), www.soc.mil/ARIS/books/pdf/14-02984_LittleGreenMen-UNCLASS-hi-res.pdf.

[32] Weissmann, “Conceptualizing and Countering Hybrid Threats and Hybrid Warfare,” 64.

силы другой страны. Именно сочетание стратегически нацеленных на население гибридных угроз и кинетических действий особенно усложняет противодействие гибридной войне и отличает её от обычной – по американской терминологии, «традиционной» – войны.

Определение гибридной войны в НАТО отражает эту сложность: там термины гибридная война, гибридные угрозы и гибридные действия часто используют взаимозаменяемо:

> Гибридные угрозы сочетают военные и невоенные, скрытые и явные средства, включая дезинформацию, кибератаки, экономическое давление, развёртывание нерегулярных вооруженных групп и применение регулярных сил. Гибридные методы используются для размывания границ между войной и миром, чтобы посеять сомнения у целевых групп населения. Они направлены на дестабилизацию и подрыв обществ.[33]

Несмотря на пересекающуюся терминологию, определение гибридной войны НАТО включает ключевые элементы как гибридных угроз, так и гибридной войны, как мы показываем тут, а именно: сочетание некинетических и кинетических действий, первоочередная задача «посеять сомнения у целевых групп населения», дальнейшая задача «дестабилизировать и подорвать общество» с конечной целью перестройки регионального и глобального порядка в пользу противника.

Эти разные определения имеют ряд общих черт, которые позволяют дать рабочее определение гибридных угроз и гибридной войны, как проявлений стратегического соперничества:

- *Участники*: Гибридные угрозы и гибридную войну могут вести как государственные, так и негосударственные игроки. Негосударственные игроки могут действовать самостоятельно или как-то сотрудничать с государствами.
- *Объекты*: Главным объектом гибридных угроз и гибридной войны является население государства. При гибридных угрозах и гибридной войне игроки используют главные уязвимости населения.
- *Характер действий*: Гибридные угрозы обычно ниже порога открытой войны. Они часто скрыты, а когда они видны, их трудно соотнести с конкретным действующим лицом, что усложняет реагирование. Гибридная война сочетает открытую войну и гибридные угрозы. Основным объектом гибридной войны тоже является население, что отличает её от обычной войны. Хотя виновник может быть известен, выработка эффективного ответа на гибридную войну и на гибридные угрозы без эскалации конфликта является сложной задачей.

[33] “Countering Hybrid Threats,” *NATO*, August 18, 2023, по состоянию на 23 января 2024, https://www.nato.int/cps/en/natohq/topics_156338.htm.

- *Задачи*: Цели гибридных угроз и гибридной войны – подорвать национальное единство, посеять раздор среди населения и поставить под сомнение легитимность власти. В конечном счёте эти действия направлены на то, чтобы вынудить власть заняться внутренними проблемами, тем самым ослабив её способность применить силу против внешнего противника.
- *Влияние на стратегическое соперничество*: В условиях стратегического соперничества, цель гибридной войны и гибридных угроз – ослабить и разделить государства и их союзы и ослабить коллективные усилия по обеспечению безопасности путём применения силы в международной системе. Это позволяет перекраивать мировой порядок в свою пользу.

Заключение

В статье утверждается, что хотя стратегическое соперничество не ново, способность государственных и негосударственных субъектов угрожать международному порядку, напрямую воздействуя на население посредством различных гибридных угроз и гибридной войны, представляет собой новое явление. Если основным объектом гибридных угроз и гибридной войны является население государства, то эффективное противодействие этим угрозам требует подготовки и обеспечения устойчивости населения к таким атакам – так называемой «стойкости общества».

Хотя тема повышения стойкости общества заслуживает отдельного глубокого исследования, статья завершается определением трёх ключевых мер, которые государства могут предпринять для повышения стойкости общества. Во-первых, правительства должны сделать приоритетом информирование и формирование устойчивости к кампаниям дезинформации и вредоносной информации, которые сегодня могут представлять собой одну из главных проблем гибридных угроз для государства. Эта большая задача охватывает широкий спектр мер, от противодействия когнитивным эффектам соцсетей и развития навыков критического мышления у населения до недопущения подрыва доверия к традиционным источникам информации, включая прессу и государственные органы.

Во-вторых, правительства должны сосредоточиться на повышении устойчивости критической инфраструктуры и ключевых служб. В базовых требованиях НАТО к устойчивости государств определены семь ключевых областей:

- Обеспечение бесперебойной работы правительства и важнейших государственных служб;
- Устойчивое энергоснабжение;
- Эффективное управление неконтролируемым перемещением людей;
- Устойчивое снабжение продовольствием и водой;
- Способность справляться с массовыми жертвами и раненными;
- Надёжные системы гражданской связи;

- Устойчивые системы гражданского транспорта.[34]

К этому списку нужно добавить способность власти давать достоверную информацию, поскольку эта способность имеет решающее значение для укрепления стойкости к дезинформации и вредоносной информации.

В-третьих, власть должна принять упреждающие меры для подготовки населения к возможности войны, включая мрачную реальность ядерного конфликта. 7 января 2024 года министр гражданской обороны Швеции Карл-Оскар Болин и главнокомандующий Микаэль Бюден публично призвали граждан Швеции морально готовиться к возможной войне, поскольку страна окончательно вступила в НАТО. Это заявление вызвало переполох в Швеции.[35] Однако подготовка населения к различным гибридным угрозам, а также к возможной войне, преднамеренно нацеленной на гражданское население, имеет важное значение для повышения устойчивости к гибридным угрозам и гибридной войне.

Это лишь три области, на которых все государства должны сосредоточиться для повышения стойкости общества с целью защиты от гибридных угроз и возможной гибридной войны. Учитывая, что население является основным объектом этих угроз, власти должны активно взаимодействовать с гражданами, чтобы смягчить воздействие гибридных угроз и подготовиться к реалиям гибридной войны.

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 **Хезер Грегг** – преподаватель нерегулярной войны/гибридных угроз в Европейском центре исследований безопасности им. Джорджа Маршалла в Гармиш-Партенкирхене, Германия, и старший научный сотрудник Института внешнеполитических исследований. Её академические интересы охватывают нерегулярную войну, гибридные угрозы, терроризм и борьбу с терроризмом, причины экстремизма и использование культуры в конфликтах с участием населения, включая укрепление стойкости и восстановление общества и национального единства после войны и политической нестабильности. *Электронная почта*: heather.gregg@marshallcenter.org

[34] Wolf-Diether Roepke and Hasit Thankey, “Resilience: The First Line of Defence,” *NATO Review*, February 27, 2019, по состоянию на 28 января 2024, www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

[35] Hope O’Dell, “Why Is Sweden Telling Its Citizens to Prepare for War?” *Chicago Council on Global Affairs*, January 24, 2024, по состоянию на 28 января 2024, https://globalaffairs.org/bluemarble/sweden-tells-citizens-prepare-war-russian-aggression-nato-membership.

Библиография

"269. Policy Planning Staff Memorandum," Office of the Historian, May 4, 1948, https://history.state.gov/historicaldocuments/frus1945-50Intel/d269.

"Countering Hybrid Threats," NATO, August 18, 2023, https://www.nato.int/cps/en/natohq/topics_156338.htm.

"Extracts from Putin's Speech at Annexation Ceremony," *Reuters*, September 30, 2022, https://www.reuters.com/world/extracts-putins-speech-annexation-ceremony-2022-09-30/.

Al-Kassab, Fatima, "What Is the 'Axis of Resistance' of Iran-Backed Groups in the Middle East?" *NPR*, October 26, 2023, https://www.npr.org/2023/10/26/1208456496/iran-hamas-axis-of-resistance-hezbollah-israel.

ARIS, *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014* (Fort Bragg, NC: The United States Army Special Operations Command, 2018), https://www.soc.mil/ARIS/books/pdf/14-02984_LittleGreenMen-UNCLASS-hi-res.pdf.

Ayres, Alyssa, "How the BRICS Got Here," Council on Foreign Relations, August 31, 2017, https://www.cfr.org/expert-brief/how-brics-got-here.

Bakir, Ali, "Turkey's Defense Industry Is on the Rise: The GCC Is One of Its Top Buyers," Atlantic Council, August 4, 2023, https://www.atlanticcouncil.org/blogs/menasource/turkey-defense-baykar-gcc-gulf/.

Barrett, Richard, Beyond the Caliphate: Foreign Fighters and the Threat of Returnees (New York, NY: The Soufan Center, October 2017), https://thesoufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf.

Borrell, Josep, "Russia Must Stop Using Food as a Weapon," European Union External Action, August 2, 2023, https://www.eeas.europa.eu/eeas/russia-must-stop-using-food-weapon_en.

Chakravorti, Bhaskar, and Gaurav Dalmia, "Is India the World's Next Great Economic Power?" *Harvard Business Review*, September 6, 2023, https://hbr.org/2023/09/is-india-the-worlds-next-great-economic-power.

Finley, Mark, and Anna B. Mikulska, "Wielding the Energy Weapon: Differences Between Oil and Natural Gas" (Houston: Rice University's Baker Institute for Public Policy, June 26, 2023), https://doi.org/10.25613/G9P2-3F78.

Galeotti, Mark, The Weaponization of Everything: A Field Guide to the New Way of War (New Haven: Yale University Press, 2022).

Garamone, Jim, "Dempsey: U.S. Forces Must Adapt to Deal with Near-Peer Competitors," Joint Chiefs of Staff, August 17, 2015, https://www.jcs.mil/Media/News/News-Display/Article/613868/dempsey-us-forces-must-adapt-to-deal-with-near-peer-competitors/.

Hoffman, Bruce, “Rethinking Terrorism and Counterterrorism Since 9/11,” *Studies in Conflict & Terrorism* 25, no. 5 (2002): 303-316, https://doi.org/10.1080/105761002901223.

Hybrid CoE, “Hybrid Threat as a Concept,” https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

Kalin, Stephen, “Gaza Diplomacy Cements Qatar’s Global Mediator Role,” *The Wall Street Journal*, November 25, 2023, https://www.wsj.com/world/middle-east/gaza-diplomacy-cements-qatars-global-mediator-role-29e0ffb7.

Kilcullen, David, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, March 2020).

Mahood, Samantha, and Halim Rane, “Islamist Narratives in ISIS Recruitment Propaganda,” *The Journal of International Communication* 23, no. 1 (2017): 15-35, https://doi.org/10.1080/13216597.2016.1263231.

Michael J. Mazarr, Bryan Frederick, and Yvonne K. Crane, Understanding a New Era of Strategic Competition (Santa Monica: RAND Corporation, November 2022), https://www.rand.org/pubs/research_reports/RRA290-4.html.

Nilsson, Niklas, et al., “Security Challenges in the Grey Zone: Hybrid Threats and Hybrid Warfare,” in *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations*, ed. Mikael Weissmann et al. (London: I.B. Tauris, 2021), 2, https://doi.org/10.5040/9781788317795.0005.

North, Douglas C., “Institutions,” *Journal of Economic Perspectives* 5, no. 1 (Winter 1991): 97-112, https://doi.org/10.1257/jep.5.1.97.

Nye, Joseph S., *Soft Power: The Means to Success in World Politics* (New York: Public Affairs Books, 2005).

O’Dell, Hope, “Why Is Sweden Telling Its Citizens to Prepare for War?” Chicago Council on Global Affairs, January 24, 2024, https://globalaffairs.org/bluemarble/sweden-tells-citizens-prepare-war-russian-aggression-nato-membership.

O’Rourke, Ronald, “Great Power Competition: Implications for Defense – Issues for Congress,” Congressional Research Services, October 3, 2023, Report, R43838, https://sgp.fas.org/crs/natsec/R43838.pdf.

Parham, Jason, “Targeting Black Americans, Russia’s IRA Exploited Racial Wounds,” Wired, December 17, 2018, https://www.wired.com/story/russia-ira-target-black-americans/.

Payne, Christian, and Lorraine Finlay, “Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack,” *The George Washington International Law Review* 49, no. 3 (2017): 535-568, https://149801758.v2.pressablecdn.com/wp-content/uploads/_pda/ILR-Vol-49.3_Panye-Finlay.pdf.

Robinson, Linda, et al., “The Growing Need to Focus on Modern Political Warfare,” Research Brief RB-10071-A (Santa Monica: RAND Corporation, 2019), https://www.rand.org/pubs/research_briefs/RB10071.html.

Roepke, Wolf-Diether, and Hasit Thankey, "Resilience: The First Line of Defence," NATO Review, February 27, 2019, https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

Thomas, Mark, "The Chinese Roots of Hybrid War-fare," CEPA, August 10, 2022, https://cepa.org/article/the-chinese-roots-of-hybrid-warfare/.

U.S. Department of Defense, "Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge," https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Wardle, Claire, "Understanding Information Disorder," *First Draft News*, September 22, 2020, https://firstdraftnews.org/long-form-article/understanding-information-disorder/.

Warner, Jason, et al., *The Islamic State in Africa: The Emergence, Evolution, and Future of the Next Jihadist Battlefront* (New York: Oxford University Press, 2021), https://doi.org/10.1093/oso/9780197639320.001.0001.

Weissmann, Mikael, "Conceptualizing and Countering Hybrid Threats and Hybrid Warfare: The Role of the Military in the Grey Zone," in *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations*, edited by Mikael Weissmann et al. (London: I.B. Tauris, 2021), 65-66, https://doi.org/10.5040/9781788317795.0011.