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

Дж. Дерлет, Дж. Пиклер, *Connections QJ* 21, № 2 (2022): 11-24
https://doi.org/10.11610/Connections.rus.21.2.01

Рецензированная статья

Угрозы XXI века требуют сдерживания XXI века

Джим Дерлет, Джефф Пиклер

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

Аннотация: В условиях соперничества США и Советского Союза (СССР) после Второй мировой войны сдерживание стало основой стратегии безопасности Соединённых Штатов. Ранее США уделяли первоочередное внимание сдерживанию обычных и ядерных угроз. Это помогло избежать прямого военного конфликта между двумя сверхдержавами, но не остановило их политическое соперничество, а лишь переместило его в сферы, снижающие риск открытого военного конфликта. Во время Холодной войны и США, и СССР прибегали к тактике нерегулярных действий для достижения своих стратегических целей в «серой зоне» ниже порога «применения силы», или «вооружённого нападения», согласно Уставу ООН. Техника ограничивала эффективность тактики нерегулярных действий, не считавшихся серьёзной угрозой национальной безопасности. Сегодня глобальная, взаимосвязанная и всепроникающая информационная среда даёт противникам множество возможностей достичь стратегических целей, не переступая стратегический порог, который в прошлом провоцировал военный ответ.

Рост числа нападений с применением нерегулярных сил показывает, что хотя сдерживание и далее позволяет избежать крупномасштабного военного конфликта между великими державами, оно не препятствует агрессии в серой зоне. От Балтики до Кавказа, Россия постоянно демонстрирует, как тактика нерегулярных действий позволяет достичь стратегических целей, не боясь неприемлемого противодействия. Тенденции мощи государств, взаимозависимость и технологии позволяют предположить, что Россия и другие противники будут и далее наращивать возможности использовать уязвимые места серой зоны. Политики сдерживания лишь обычными и ядерными силами уже недостаточно. Чтобы сдержать тактику нерегулярных действий,

США должны выработать стратегию сдерживания XXI века. Такая необходимость только вырастет с попытками России компенсировать свои военные неудачи в Украине. С ослаблением российских неядерных сил Россия всё больше будет применять тактику нерегулярных действий для ударов по противникам. В этом исследовании рассмотрено снижение актуальности традиционных стратегий ядерного и неядерного сдерживания и показано, что сдерживание пора изменить для противодействия угрозам XXI века.

Ключевые слова: сдерживание, Россия, гибридные угрозы, нерегулярные боевые действия, серая зона, национальная безопасность.

Вступление

Вскоре после поражения Германии во Второй мировой войне США и СССР втянулись в глобальную борьбу за власть и влияние. В отличие от предыдущих споров великих держав, часто приводивших к вооружённым конфликтам, ядерное оружие изменило калькуляции риска для обеих сторон. Это имело четыре важных последствия. Во-первых, чтобы снизить вероятность конфликта и эскалации, США и СССР прибегали к тактике нерегулярных действий.[1] Во-вторых, это перенесло соперничество в серую зону ниже уровня традиционного межгосударственного конфликта.[2] В-третьих, поскольку боевые действия между ядерными противниками могут привести к их взаимному уничтожению, военную силу могли применять преимущественно для «принуждения, запугивания и сдерживания».[3] В-четвёртых, как показал Вьетнам и Афганистан, это перенесло вооружённый конфликт на уровень марионеток соперников.

В результате в США была принята политика сдерживания. Её принятие серьёзно изменило вооружённые силы. Ядерный стратег Бернард Броди писал: «до сих пор главной целью нашего военного ведомства была победа в войне, теперь его главной целью должно стать её предотвращение».[4] Есть

[1] В тактике нерегулярных действий используются классические принципы стратегии – победа без войны, довоенные меры и «тактика салями». Современные примеры включают дезинформацию, кибератаки, экономическое принуждение, юридическое крючкотворство и использование марионеток.

[2] Kathleen H. Hicks, “Russia in the Grey Zone,” Commentary (Washington: Center for Strategic & International Studies, July 25, 2019), https://www.csis.org/analysis/russia-gray-zone.

[3] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 2008), 34. Цель сдерживания – предотвратить потенциальные действия агрессора, убедив его в том, что издержки или последствия его действий перевешивают любые потенциальные выгоды. Это определение основано на классических взглядах на теорию и практику сдерживания.

[4] Andrew F. Krepinevich Jr., “The Eroding Balance of Terror: The Decline of Deterrence,” *Foreign Affairs* (January/February 2019), https://www.foreignaffairs.com/eroding-balance-terror.

два традиционных вида сдерживания: сдерживание недопущением и сдерживание возмездием. Сдерживание недопущением основано на способности удержать от действий, сделав их успех маловероятным. Сдерживание возмездием – это угроза создать издержки: экономические, военные, политические, или все вместе, превосходящие возможные выгоды агрессии. Эффективное сдерживание недопущением или возмездием обусловлено чёткой формулировкой национальных интересов («красных линий»), способностью осуществить свои угрозы, верой в готовность реализовать их и связью с противником, чтобы тот понимал соотношение издержек и выгод своих действий.[5] Обычное и ядерное сдерживание стало основой безопасности США на последующие 50 лет – Соединённые Штаты старались достичь своих стратегических целей, в то же время избегая полномасштабной войны.

Нерегулярные угрозы и сдерживание

Сдерживание времён Холодной войны было эффективным, потому что внешняя политика США удерживала стратегическое соперничество ниже порога войны между государствами. Но ядерное сдерживание долго приводило к тому, что Гленн Снайдер назвал парадоксом стабильности-нестабильности. «Это означает, что чем стабильнее ядерный баланс, тем охотнее державы будут вступать в конфликты ниже порога войны».[6] Так было во время Холодной войны, так это и сегодня. В докладе Госдепартамента 1981 г. отмечены иррегулярные действия Советского Союза, включая «контроль прессы в зарубежных странах; открытую или частичную подделку документов; слухи, инсинуации, передёргивание фактов и ложь; использование подставных международных и местных организаций; тайную работу радиостанций; привлечение к сотрудничеству научных, политических, эконо-

[5] Если раскрыть эти три ключевых аспекта сдерживания, способность – это возможность влиять на поведение. Для эффективного сдерживания нужен ряд возможностей, гарантирующих, что любой вид агрессии не достигнет цели и/или будет сопряжён с реальным риском неприемлемых последствий для противника. Вера основана на поддержании уверенности в том, что заявленные меры сдерживания действительно будут реализованы. Вера требует наличия возможности реализовать множество вариантов и готовности их использовать. Связь означает донесение нужного месседжа до противника, которого требуется сдержать. Эффективная связь требует решимости не допустить никаких выгод и/или создать издержки при любых агрессивных действиях.

[6] Glenn Snyder, *The Balance of Power and the Balance of Terror*, quoted in Michael Kofman, "Raiding and International Brigandry: Russia's Strategy for Great Power Competition," *War on the Rocks*, June 14, 2018, https://warontherocks.com/2018/ 06/ raiding-and-international-brigandry-russias-strategy-for-great-power-competition/.

мических и медийных деятелей страны для влияния на политику государства».[7] Эти усилия не дали существенного стратегического эффекта из-за ограничений информационных технологий и биполярной геополитической ситуации того времени. Сегодня из-за изменений в глобальном балансе сил, возникновения многополярной системы, технологий, позволяющих государствам напрямую использовать уязвимость и взаимозависимость общества, государства гораздо более уязвимы к тактике нерегулярных действий. Вмешательство России в президентские выборы в США в 2016 г. и утечка данных SolarWinds в 2020 г. показывают, что наши противники могут достичь своих стратегических целей с низкими затратами и ограниченным риском установления виновных или эскалации.

Несмотря на эти изменения, подход США к сдерживанию остается в целом таким же, как и во время Холодной войны. Основное внимание уделяется использованию обычных и ядерных сил для сдерживания и, при необходимости, поражения равного противника на поле боя. В текущих усилиях по модернизации армии, США отдают приоритет летальности на поле боя, вкладывая миллиарды долларов в высокоточные средства поражения большой дальности, боевые машины следующего поколения, будущие платформы вертикального взлёта, модернизацию армейских сетевых технологий, систем ПВО и ПРО, а также увеличение возможностей индивидуального вооружения солдат. Обучение и учения по-прежнему сосредоточены на сближении с равным противником и его уничтожении при помощи точного огня и манёвра. Хотя мощные и обученные обычные и современные ядерные силы обеспечивают сдерживание, последние 15 лет показали, что они не могут сдержать кибератаки, использование марионеток, дезинформацию и другую тактику нерегулярных действий, доминирующую в современном стратегическом противоборстве. Наши же противники учли изменения стратегической ситуации в своей военной стратегии. Так, начальник Генерального штаба Вооруженных Сил Российской Федерации Герасимов отмечал, что «правила войны» изменились: «Возросла роль невоенных способов в достижении политических и стратегических целей, которые в ряде случаев по своей эффективности значительно превзошли силу оружия».[8]

Как отмечал в своей книге *The Weaponisation of Everything* Марк Галеотти, «мир сейчас более сложен и, главное, теснее взаимосвязан, чем когда-

---

[7] "Soviet 'Active Measures': Forgery, Disinformation, Political Operations," Special Report No. 88 (Washington, DC: U.S. Department of State, Bureau of Public Affairs, October 1981), http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20Forgery,%20Disinformation,%20Political%20Operations%20October%201981.pdf.

[8] Валерий Герасимов, «Ценность науки в предвидении: Новые вызовы требуют переосмыслить формы и способы ведения боевых действий», *Военное обозрение* (январь-февраль 2016): 30-38, 24, https://web.archive.org/web/20170820160806/http://www.vpk-news.ru/articles/14632.

либо прежде… Войны без войны, невоенные конфликты, в которых используются все прочие средства, от подрывной деятельности до санкций, от мемов до убийств, могут стать новой нормой».[9] Эта новая стратегическая ситуация подрывает нашу нынешнюю стратегию сдерживания. «…развитие событий ведёт к неизбежному и тревожному выводу: главной стратегической проблемой нынешней эпохи является не возобновление соперничества великих держав и не распространение передовых вооружений. Это упадок сдерживания».[10] Эта ситуация имеет далеко идущие последствия для национальной безопасности. Главное – она подрывает обычное и ядерное сдерживание и позволяет противникам действовать безнаказанно.[11] Чтобы изменить ситуацию, нам нужно изменить расчёт издержек и выгод для России и других противников. Иными словами, мы должны создать стратегию сдерживания нерегулярных угроз.

Комплексное сдерживание

Противники применяют летальную и нелетальную тактику нерегулярных действий для достижения своих целей. Примеры включают использование марионеток, угрозы критически важной инфраструктуре, гражданам (убийства, преследования, похищения людей и т.д.), вмешательство в демократические и управленческие функции. Поэтому для национальной безопасности США важна способность сдержать нерегулярные угрозы. Во временных стратегических директивах по национальной безопасности на 2021 г. президент Байден пообещал «развивать возможности для лучшего противостояния и сдерживания в серой зоне».[12] После назначения на пост министр обороны США Остин заметил, что Соединенным Штатам нужен новый подход к сдерживанию, который бы «при необходимости создавал издержки, используя при этом все наши инструменты для снижения риска эскалации с противниками и реагирования на вызовы ниже уровня вооруженного конфликта». Эту новую политику назвали «комплексным сдерживанием».[13]

---

9 Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War* (New Haven, CT: Yale University Press, 2022), 18.

10 Krepinevich Jr., "The Eroding Balance of Terror."

11 Sean Monaghan, "Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice," Hybrid CoE Paper 12 (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, March 31, 2022), 17, https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/.

12 President of the United States, "Interim National Security Strategic Guidance" (Washington, D.C.: The White House, March 2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

13 Lloyd Austin, "Message to the Force" (Washington, D.C.: Office of the Secretary of Defense, March 4, 2021), https://media.defense.gov/2021/Mar/04/2002593656/-1/-1/0/SECRETARY-LLOYD-J-AUSTIN-III-MESSAGE-TO-THE-FORCE.PDF.

Заместитель министра обороны по вопросам политики Колин Каль охарактеризовал комплексное сдерживание как осведомлённость «почти обо всем, что мы делаем… интегрированная во всех сферах – обычной, ядерной, кибер, космической, информационной, на всех театрах военных действий и потенциальных конфликтов, интегрированная во всем спектре конфликта, от войны высокой интенсивности до серой зоны». Комплексное сдерживание также предусматривает объединение всех элементов власти государства. Каль отметил, что хотя сдерживание служит основой стратегии США со времен Холодной войны, оно имеет другое значение, как часть комплексного сдерживания: «нам нужно думать о сдерживании по-другому, учитывая существующую обстановку в области безопасности и возможные сценарии конфликта, который мы пытаемся предотвратить… Министерство обороны должно иметь возможности и концепции, чтобы не дать свершиться сценариям, которые, как мы знаем, замышляют потенциальные противники».[14]

Хотя компоненты комплексного сдерживания еще полностью не отработаны, стратегия сдерживания нерегулярных угроз должна включать возможность как «наказать» государство-агрессор, использующее тактику нерегулярных действий, так и «лишить» его возможности существенно повлиять на государство, подвергшееся нападению.[15] Как и традиционное сдерживание, комплексное сдерживание предусматривает определение и доведение до противника «красных линий». Эти красные линии должны определяться тем, что страна не может сдержать все нерегулярные нападения. Вместо этого следует сосредоточиться на наиболее опасных из них, понимая, что это также может быть приглашением к использованию уязвимых мест. После выявления угроз государства должны иметь возможность наказать противника. При этом следует исходить из того, чего не желает противник. Иными словами, подвергшиеся нападению государства должны иметь возможность поразить уязвимые места или основные интересы противника. Важно отметить, что контрмеры могут быть либо аналогичными (ответ на кибератаки кибератаками), либо ответ может быть дан вне сферы, в ко-

[14] Cited in Jim Garamone, “Concept of Integrated Deterrence Will Be Key to National Defense Strategy, DOD Official Says,” *U.S. Department of Defense News*, December 8, 2021, www.defense.gov/News/News-Stories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/.

[15] Есть две устоявшиеся теории сдерживания нерегулярных угроз: одна – сдерживание возмездием, другая основана на сдерживании недопущением. См. Dorthe Bach Nyemann and Heine Sørensen, “Going Beyond Resilience: A Revitalized Approach to Counter Hybrid Threats,” Hybrid CoE Strategic Analysis 13 (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, January 2019), https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-13-going-beyond-resilience-a-revitalised-approach-to-countering-hybrid-threats/, и Monaghan, “Deterring Hybrid Threats.” В работе утверждается, что эффективная стратегия сдерживания нерегулярных угроз должна включать элементы обеих.

торой совершена акция. Примером может служить угроза финансовых санкций в случае кибератаки.[16] Для меньшего государства возможно коллективное возмездие агрессору со стороны альянса (ЕС, НАТО), членом которого оно является.

Второй компонент комплексной стратегии сдерживания – способность подвергшихся нападению государств не дать противнику воспользоваться преимуществами нерегулярного удара. Это можно сделать, повышая стойкость общества.[17] В Евросоюзе стойкость определяют как «способность противостоять давлению и восстанавливаться, усиливаясь после сложностей».[18] Меры стойкости обычно недороги и вписываются в распространённые парадигмы «управления рисками» национальной безопасности.[19] Поскольку характер нерегулярных угроз (неопределённость, сложность выявления и атрибуции) усложняет сдерживание через возмездие, важно, чтобы государства сами становились менее уязвимыми к ним. Элемент недопущения комплексной стратегии сдерживания на основе стойкости позволяет государствам лучше использовать ограниченные ресурсы, выявляя и усиливая слабые места общества. Стойкость также укрепляет основы стратегии сдерживания (связь, способность, веру). В целом, комплексная стратегия

---

[16] Vytautas Keršanskas, “Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats,” Hybrid CoE Paper 2 (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, March 2020), 12, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf.

[17] Tim Prior, “Resilience: The ‘Fifth Wave’ in the Evolution of Deterrence,” Chapter 4 in *Strategic Trends 2018*, ed. Oliver Thränert and Martin Zapfe (Zurich: Center for Security Studies, 2018), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ST2018-06-TP.pdf); Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, Research Report RR-2942-OSD (Santa Monica, CA: RAND, 2019), https://www.rand.org/pubs/research_reports/RR2942.html; и Elizabeth Braw, *The Defender’s Dilemma: Identifying and Deterring Gray-Zone Aggression* (Washington, D.C.: American Enterprise Institute, 2021), https://www.aei.org/the-defenders-dilemma/.

[18] European Commission, “Joint Framework on Countering Hybrid Threats: a European Union Response,” Joint Communication to the European Parliament and the Council (Brussels, April 6, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018&from=EN. Хотя стойкость сама уже стала популярной стратегией и применяется для рационализации различных вариантов политики, повышение стойкости должно основываться на оценке секторов общества, наиболее уязвимых для нерегулярных угроз. В зависимости от выявленной уязвимости, повышение устойчивости может включать усиление кибербезопасности, совершенствование инфраструктуры, обучение противодействию дезинформации, диверсификацию ресурсов, антикоррупционные программы и т. д.

[19] Albin Aronsson, “The State of Current Counter-Hybrid Warfare Policy,” Information note, Multinational Capability Development Campaign (MCDC), MCDC Countering Hybrid Warfare Project, March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803970/20190519-MCDC_CHW_Info_note_10-State_of_current_policy.pdf.

сдерживания должна быть нацелена на то, чтобы помешать враждебным государствам использовать тактику нерегулярных действий, одновременно смягчая последствия их возможного применения. Эта стратегия должна ограничить оперативный простор для нерегулярных действий и отбить охоту к ним.[20]

Разработка стратегии, удерживающей потенциальных противников от применения тактики нерегулярных действий путём возмездия и недопущения, станет важным элементом стратегии сдерживания XXI века. Во всё более туманном промежутке между войной и миром государства должны быть способны чётко донести до потенциального агрессора, что его обычные, ядерные *и* нерегулярные угрозы не принесут успеха. В сдерживание будут верить, только если у США и их союзников будет возможность и воля чётко донести свою готовность наказать и воспрепятствовать нерегулярным действиям противника. В настоящее время тут имеется пробел в американской политике сдерживания, который нужно восполнить. В следующем разделе рассматриваются мероприятия союзников и партнёров, направленные на повышение их способности сдерживать нерегулярные угрозы.

Военный компонент комплексного сдерживания

Из-за характера нерегулярных угроз, комплексная стратегия сдерживания требует участия всего общества, координирующего гражданские [21] и военные элементы власти государства в разных сферах. Всё больше стран включают в свою стратегию национальной безопасности концепцию «тотальной

[20] Nyemann and Sørensen, “Going Beyond Resilience: A Revitalized Approach to Counter Hybrid Threats.”

[21] В дополнение к традиционным гражданским структурам национальной безопасности, таким, как министерства иностранных и внутренних дел, службы разведки и безопасности и т.д., крайне важно привлечь науку, неправительственные организации, бизнес, средства массовой информации и отдельных граждан. Последние часто обладают знаниями, возможностями и способностями по противодействию незаконным угрозам, которых нет у правительственных учреждений.

обороны»[22] для снижения нерегулярных угроз.[23] Финляндия, Швеция, страны Балтии считают стратегию тотальной обороны наилучшим методом сдерживания широкого спектра угроз.

Признавая, что для снижения нерегулярных угроз необходимо участие всего общества, мы сосредоточимся на роли военных. В частности, на действиях, предпринимаемых вооруженными силами союзников и партнёров для обучения своих граждан, развития новых возможностей, создания соответствующих оргструктур и организации учений, точно отражающих реальные угрозы и предоставляющих возможность общественным организациям и отдельным лицам участвовать своими силами и возможностями в противодействии нерегулярным угрозам.

Чтобы гражданское общество могло эффективно участвовать в тотальной обороне, оно должно понимать свою роль в ней. Финские военные проводят ежегодный «Курс национальной обороны», где участников знакомят с угрозами, политикой безопасности и обороны, а также их ролью в укреплении национальной безопасности. Курс также помогает наладить сотрудничество и связи между руководителями бизнеса, правительства и общества.[24] В поддержку стратегии тотальной обороны литовские военные помогли развернуть кампанию по разоблачению российской дезинформации. Силами Командования стратегических коммуникаций в Литве создана общая платформа для выявления дезинформации, её изобличения фактами и доведения этой информации до общества. Эта программа играет важную роль в просвещении общества и отражении дезинформационных атак, способствуя обмену информацией между заслуживающими доверия медиаплатформами.[25]

---

[22] Тотальная оборона – это участие всего общества в обеспечении национальной безопасности. Его цель – сдержать потенциального противника путём повышения издержек агрессии и снижения шансов на её успех. Тотальная оборона мобилизует все гражданские и военные ресурсы государства, чтобы противник столкнулся с национальным сопротивлением в случае нападения или с неуправляемой страной при оккупации. Концепция тотальной обороны не нова. Такой была политика безопасности некоторых неприсоединившихся стран во время Холодной войны. Её главная черта – организованное взаимодействие государственных органов, гражданских организаций, частного сектора и широкой общественности. Поскольку нынешние нерегулярные угрозы включают как военные, так и невоенные вызовы, а грань между войной и миром размыта, важен комплексный подход. Тотальную оборону отличает от традиционного сдерживания и обороны прямое участие гражданского общества.

[23] Tom Rostoks, "The Evolution of Deterrence from the Cold War to Hybrid War," in *Deterring Russia in Europe: Defence Strategies for Neighbouring States*, ed. Nora Vanaga and Toms Rostoks (London: Routledge, 2018), https://doi.org/10.4324/9781351250641.

[24] Braw, *The Defender's Dilemma*, 179.

[25] Benas Gerdziunas, "Lithuania: The War on Disinformation," *Deutsche Welle*, September 27, 2018, www.dw.com/en/lithuania-hits-back-at-russian-disinformation/a-45644080.

Что касается новых возможностей, то Эстония использует для усиления киберзащиты призыв. Набирая в вооруженные силы киберспециалистов с высшим образованием, Эстония существенно повышает военные кибервозможности и укрепляет киберинфраструктуру после возвращения призывников к гражданской жизни.[26] Это также даст Эстонии подготовленный и опытный киберрезерв, обученный реагировать на чрезвычайные кибер-ситуации. Вооруженные силы Эстонии также спонсируют добровольческое подразделение киберзащиты (CDU). Оно проверяет и даёт допуск членам, обеспечивая тем самым дополнительные возможности защиты от киберугроз.[27] Обе эти программы дают экспертные знания, улучшающие сдерживание кибератак.

Сдерживание нерегулярных угроз также требует соответствующих бюрократических структур. Комитет безопасности Министерства обороны Финляндии объединяет правительственные учреждения и неправительственные организации, чтобы обойти типичные бюрократические проблемы, быстро обмениваться информацией, координировать ответные меры и информировать население Финляндии о нерегулярных угрозах и нападениях.[28] Комитет безопасности включает примерно 30 специалистов, представляющих всё финское общество, и занимается обучением государственных служащих и журналистов тактике дезинформации на семинарах и тренингах. Комитет собирается не реже раза в месяц, чтобы «гарантировать, что жизненно важная информация не будет ограничена правительственными учреждениями или частным сектором».[29] Когда российские СМИ обвинили финское правительство в похищении детей русского происхождения в борьбе за опеку между финнами и русскими, комитет сотрудничал с правительственными чиновниками, чтобы развеять эту ложь. Такая бюрократическая структура помогает отражать информационные атаки, повышая способность правительства выявлять, а населения – игнорировать их.

Эти примеры показывают, как стратегия тотальной обороны может улучшить защиту от нерегулярных угроз, но её эффективность можно определить только на учениях. В отличие от опыта США, союзники и партнёры имеют обширный опыт привлечения гражданских структур (бизнеса, НПО и

---

[26] Adi Gaskell, “How Estonia Is Using Military Service to Bolster Cybersecurity Skills,” *Cybernews*, September 28, 2021, https://cybernews.com/security/how-estonia-is-using-military-service-to-bolster-cybersecurity-skills/.

[27] “Cyber Security in Estonia 2020” (Tallinn: Information System Authority, 2020), accessed December 21, 2021, https://www.ria.ee/sites/default/files/cyber_aastaraamat_eng_web_2020.pdf.

[28] Mackenzie Weinger, “What Finland Can Teach the West About Countering Russia’s Hybrid Threats,” *World Politics Review*, February 13, 2018, https://www.worldpoliticsreview.com/articles/24178/what-finland-can-teach-the-west-about-countering-russia-s-hybrid-threats.

[29] Weinger, “What Finland Can Teach the West About Countering Russia’s Hybrid Threats.”

т.д.) к противодействию нерегулярным угрозам. Так, литовские военные регулярно проводят учения для всего общества, что позволяет различным группам подготовиться к нерегулярным угрозам и реагировать на них. В этих учениях участвовали представители транспорта, связи, энергетики, инфраструктуры, правоохранительных органов и вооруженных сил. Примечательно, что некоторые учения требуют координации в условиях отсутствия сотовой связи, когда и военные, и гражданские системы связи не работают.[30] В шведских учениях «Total Defense 2020» приняли участие более 60 государственных ведомств и неправительственных организаций. Эти учения включали множество сценариев угроз и предоставили гражданским организациям и государственным чиновникам на местном, региональном и национальном уровне возможность отработать реакцию на разные типы нерегулярных атак – от кибератак до прокси-вторжения.[31] Подобные учения улучшают сдерживание недопущением, демонстрируя противнику, что атаки будут неэффективными.

EUCOM и комплексное сдерживание

Учась у союзников и партнёров, которые годами сталкиваются с нерегулярными угрозами, Европейское командование США (EUCOM) должно включить аналогичные действия в комплексную, скоординированную и интегрированную стратегию сдерживания нерегулярных атак. Как отмечалось выше, этот тип стратегии требует интеграции всех компонентов государственной власти. В этом разделе рассмотрены методы обучения EUCOM своего персонала, поиска и интеграции новых возможностей, создания соответствующих структур и организации учений по улучшению защиты от двух, вероятно, наиболее распространенных нерегулярных угроз: дезинформации и киберугроз. Эти рекомендации можно быстро реализовать с минимальными изменениями в оргструктуре EUCOM. Главное – они будут способствовать субконвенциональному сдерживанию, устраняя конкретные уязвимости, которые Россия продолжает атаковать практически безнаказанно.

В настоящее время EUCOM отрабатывает оперативные планы на стратегических круглых столах, посвящённых России, под руководством боевого командира. Командующий EUCOM отметил, что эти круглые столы «играют важную роль в обеспечении стратегической и оперативной синхронизации между высшими военными руководителями нашей страны по ключевым вопросам, связанным с глобальными кампаниями и соперничеством». Од-

[30] BNS, “Drills Will Allow Better Preparation for Hybrid Threats – Transport Minister,” *The Lithuania Tribune*, February 28, 2018, https://lithuaniatribune.com/drills-will-allow-better-preparation-for-hybrid-threats-transport-minister/.

[31] Swedish Armed Forces, “Total Defence Exercise 2020,” September 17, 2021, www.forsvarsmakten.se/en/activities/exercises/total-defence-exercise-2020/.

нако, ограничивая участие высокопоставленными представителями Министерства обороны, эти стратегические круглые столы не включают важных представителей промышленности и других правительственных и неправительственных организаций Европы. Подобно Комитету по безопасности Министерства обороны Финляндии, на эти круглые столы следует приглашать ключевых региональных невоенных заинтересованных участников, давая участникам более полное понимание российской дезинформации и киберугроз, а также выявляя возможности и потенциал общества для смягчения их последствий. Превращение посвящённого России стратегического круглого стола в образовательное мероприятие для заинтересованных сторон привнесет в группу уникальные мнения и опыт, которые в противном случае не были бы включены во встречу одних только военных.

Что касается возможностей, то в США киберсдерживание осуществляет почти исключительно Киберкомандование США. Развертывание их «кибероотрядов» в Литве для «киберзащиты» от агрессии России улучшает киберосдерживание, но одновременно демонстрирует ограниченные кибервозможности EUCOM.[32] Инициатива, аналогичная эстонскому подразделению киберзащиты, помогла бы EUCOM усилить возможности киберсдерживания за счет привлечения гражданских специалистов по кибербезопасности. EUCOM мог бы проводить проверки и выдавать допуски для усиления возможностей борьбы с киберугрозами. Это не только улучшит киберсдерживание EUCOM, но и поможет включать кибероперации в планирование и оперативную деятельность, предоставив командующему больше возможностей для противодействия многочисленным угрозам в киберсфере.

Усиленные возможности дадут ограниченный сдерживающий эффект, если они не интегрированы в планирование и операции. Печалясь об отсутствии эффективной структуры для интеграции информационных операций, директор Объединенного штаба США по командованию, управлению, связи и компьютерным/кибертехнологиям недавно отметил, что «боевые командиры слишком часто думают об информационных операциях в последнюю очередь. Мы очень хорошо понимаем активные операции. В культурном отношении мы не доверяем некоторым методам проведения информационных операций (ИО). Идея заключается в том, чтобы «добавить немного ИО». Командиры должны проводить информационные операции – как и активные операции – для подготовки поля боя».[33] Для более эффективной интеграции информационной работы в военные операции необходимо создать объединенную ячейку информационной войны, где будут работать граж-

[32] Colin Demarest, “US Cyber Squad Boosts Lithuanian Defenses amid Russian Threat,” *C4ISRNET*, May 5, 2022, https://www.c4isrnet.com/cyber/2022/05/05/us-cyber-squad-boosts-lithuanian-defenses-amid-russian-threat/.

[33] Stew Magnuson, “U.S. Still Playing Catchup in Information Operations,” *National Defense Magazine*, February 11, 2022, www.nationaldefensemagazine.org/articles/2022/2/11/still-playing-catch-up-in-information-operations.

данские и военные специалисты. Эта ячейка могла бы выявлять дезинформацию и противодействовать ей. Сейчас информационные эксперты Командования ВС США в Европе рассредоточены по штабам в зависимости от их специализации, спрятаны в секретных комнатах, в бункерах или похоронены в особом отделе штаба. Поскольку информация является объектом нерегулярных атак, опыт информационной войны не может храниться в нескольких кабинетах и быть скрыт грифом секретности. Объединенная ячейка позволит EUCOM более эффективно выявлять и сдерживать информационные угрозы России.

Совершенствование подготовки, возможностей и структур будет иметь ограниченный эффект без проверки на учениях. EUCOM и подчиненные командования ежегодно проводят около 30 учений, уделяя особое внимание взаимодействию США, союзников и партнёров. Эти учения способствуют обычному и ядерному сдерживанию, демонстрируя военную мощь США и их приверженность союзническим обязательствам и партнёрству. Однако они мало помогают сдерживанию нерегулярной агрессии. Дело в том, что нынешние учения ориентированы на летальные операции, не учитывают нерегулярные угрозы и не обеспечивают эффективного участия других правительственных учреждений, частного бизнеса или неправительственных организаций. Командованию ВС США в Европе следует включать нерегулярные угрозы в сценарии учений и привлекать широкий круг участников для оценки нашей способности отражать нерегулярные атаки, особенно кибернетические и информационные. Учения такого типа ясно показали бы нашу силу и продемонстрировали нашу способность выявлять и ослаблять российскую тактику нерегулярных действий, тем самым помогая сдерживанию.

Перемены – это всегда вызов, и военные структуры и организации особенно противятся им. Тем не менее перемены необходимы, чтобы помочь сдерживанию в XXI веке. Хотя из-за вторжения России в Украину возобновилось обсуждение боевых действий с применением обычного и ядерного оружия, эта точка зрения недальновидна. Российская армия подвергается уничтожению, и аналитики считают, что пройдут годы, прежде чем она станет смертельной угрозой для НАТО. Однако российские стратегические интересы не изменятся, и Россия продолжит использовать тактику нерегулярных действий против Соединенных Штатов, их союзников и партнёров по мере восстановления своего военного потенциала. Пока русские глубоко увязли в Украине, у Командования ВС США в Европе есть уникальная возможность улучшить сдерживание нерегулярной агрессии.

Заключение

Ядерная триада, сильная система альянсов и технологически развитые вооруженные силы продолжают сдерживать обычное и ядерное нападение России на Соединенные Штаты. Тем не менее продолжающийся рост числа

нерегулярных нападений показывает, что нынешняя стратегия сдерживания США не смогла их предотвратить. В отличие от Холодной войны, тактика нерегулярных действий напрямую угрожает национальной безопасности, подрывая сдерживание и дестабилизируя общество. Поэтому политика сдерживания, ориентированная исключительно на обычные и ядерные силы, уже не достаточна.

Размышляя о сдерживании, бывший заместитель генерального секретаря НАТО Вершбоу отметил, что сдерживание «требует эффективных, устойчивых возможностей и чёткой позиции, которая не оставит противнику сомнений в том, что он потеряет больше, чем выиграет от агрессии, будь то внезапное обычное нападение, первое применение ядерного оружия для деэскалации обычного конфликта, кибератака на критическую инфраструктуру или нерегулярная кампания по дестабилизации обществ союзников». Наша нынешняя политика сдерживания не полностью учитывает изменения оперативной обстановки. Для укрепления национальной безопасности Соединенным Штатам нужна стратегия сдерживания XXI века, чтобы сдержать угрозы XXI века.

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. 21, 2022, вышел при поддержке правительства США.

Об авторах

Д-р **Джим Дерлет** – преподаватель нерегулярных боевых действий и директор курсов семинара по нерегулярным боевым действиям/ гибридным угрозам в Европейском центре исследований в области безопасности им. Джорджа Маршалла.
Электронная почта: James.Derleth @marshallcenter.org

Полковник **Джефф Пиклер** – штатный преподаватель Европейского центра исследований в области безопасности им. Джорджа Маршалла.
Электронная почта: Jeffrey.Pickler@marshallcenter.org