



Сдерживание гибридной войны: подходы НАТО к российским диверсиям

Анка Иоана Анеску

Выпускница Европейского центра исследований в области безопасности им. Джорджа Маршалла, Германия, <https://www.marshallcenter.org>

Аннотация: В статье представлен сравнительный анализ понимания и применения концепции сдерживания, с особым акцентом на её роль в гибридной войне, в Российской Федерации (действие до противодействия, принудительная эскалация), в отличие от подхода НАТО, основанного на предотвращении агрессии посредством надежного сдерживания и коллективной стойкости. Основываясь на этом сравнении, статья рассматривает стратегии сдерживания НАТО российской гибридной войны, уделяя особое внимание диверсиям, как ключевому асимметричному инструменту, уходящему корнями в тайные практики советской эпохи и возрождённому в последние годы на фоне эскалации угроз в «серой зоне», особенно после вторжения в Украину и атак на стратегическую инфраструктуру НАТО.

На основе комплексной методологии, сочетающей исторический анализ, теоретическую базу, тематические исследования недавних инцидентов (2022–2025 гг.), теоретическое моделирование и оценку политики, в исследовании утверждается, что эффективное противодействие диверсиям в гибридной войне может обеспечить лишь комплексное сдерживание. Такой подход должен включать заблаговременное стратегическое прогнозирование на основе исторических закономерностей и прецедентов, расширенный обмен разведданными, устойчивость инфраструктуры и применение принципа обороны силами всего общества. В целом, в статье утверждается, что НАТО и страны-союзники должны перейти от реагирования к предупреждению в обороне и сдерживании, сочетая стратегическое прогнозирование с гибкими оборонными возможностями.

Ключевые слова: сдерживание, гибридные угрозы, обычная война, нерегулярная война, диверсии.

Сдерживание с исторической и теоретической точек зрения

Сдерживание определяется в двух основных контекстах: (1) предотвращение каких-то действий, например, сдерживание преступности, и (2) в политике – политика создания значительного военного потенциала для предотвращения нападения других стран.¹

В XVI веке крестьяне Зальцбурга восстали против непомерных налогов и бесправия, взбунтовавшись против богатых князей-архиепископов, и попытались захватить город. Не сумев преодолеть стены крепости Хоэнзальцбург, они осадили её в надежде вынудить защитников сдаться, заморив их голодом. Поскольку запасы продовольствия были на исходе, и остался всего один бык, город прибег к хитроумной уловке: коричневого пятнистого быка провели вдоль крепостных стен, на следующий день его вымыли и покрасили в белый цвет, а ещё через день – в чёрный, создав видимость наличия множества здоровых животных. Обманутые осаждающие, думая, что в городе ещё много еды, отказались от своих планов и отступили. Обман оказался настолько эффективным, что превратился в местную легенду – бесмертную историю о сдерживании и психологической войне.²

Эта легенда показывает, что понятие сдерживания имеет глубокие исторические корни и существовало задолго до появления официального определения. Ранние формы сдерживания можно увидеть в таких практиках, как феодальные союзы (через браки и клятвы верности), строительство замков и укреплений, демонстрация военной силы на парадах и турнирах, а также публичное наказание преступников. В ранних формах экономических санкций государства отказывались торговать с агрессорами, чтобы предотвратить враждебные действия.

Вообще сдерживание является одним из основополагающих аспектов человеческого поведения и социализации, который начинается в раннем детстве. С раннего возраста люди учатся избегать определённых действий из-за угрозы последствий, таких как наказание или боль. Так, родители учат детей не совершать опасных или неподобающих поступков, предупреждая, запрещая и наказывая. Таким образом, сдерживание – это универсальный, инстинктивный человеческий акт, который люди понимают с раннего возраста и используют в повседневной жизни как для самозащиты, так и для влияния на других людей, независимо от своего социально-культурного окружения. Эта универсальность объясняет, почему сдерживание работает в самых разных ситуациях, от элементарных личных отношений до институциональной политики безопасности.

Понятие *сдерживания* (*deterrence*), произошедшее от латинского слова *terrere* («пугать»), касается рациональной стратегии использования угрозы

¹ Lawrence Freedman, *Deterrence* (Cambridge, MA: Polity Press, 2004).

² “‘Salzburger Bierfleisch’ and the Legend of the Bull Washers,” *Salzburg.info*, www.salzburg.info/en/magazin/art-culture/salzburger-bierfleisch-and-the-legend-of-the-bull-washers_a_445970.

наказания и ответной эмоциональной реакции для предотвращения нежелательных или враждебных действий. Помимо межличностного аспекта, сдерживание во взаимоотношениях существовало при разных формах социальной и политической организации, от племен до государств и наднациональных образований. Его формализовали и описали как теоретическую стратегию такие ученые, как Томас Шеллинг (1960; 1966) и Герман Кан (1962), особенно применительно к безопасности в эпоху Холодной войны (1947–1991),³ в связи с гонкой ядерных вооружений. В частности, теория сосредоточилась на отношениях США с СССР в условиях угрозы и логики взаимного гарантированного уничтожения.

Позже, после падения коммунистической системы в Европе и в постсоветскую эпоху (1990-е – 2000-е гг.), теорию сдерживания адаптировали для устранения неядерных и негосударственных угроз, включая терроризм и кибератаки. Сегодня сдерживание стало ключевым компонентом киберзащиты, правоохранительной деятельности и борьбы с терроризмом, охватив сферы цифровой, гибридной и асимметричной войны.

В сфере безопасности сдерживание означает предотвращение или ограничение действий противника – обычно агрессивных или направленных на причинение стратегического ущерба, гибель и/или ранение людей – угрозой серьёзных последствий.⁴ Часто оно предполагает угрозу ответных мер (страх последствий) или демонстрацию способности нанести чрезвычайно серьёзный ущерб, что снижает ожидаемую выгоду от таких действий. По сути, чтобы сдержать противника, нужно убедить его в том, что риски и убытки от его действий, вероятно, превысят выгоды. Сдерживание часто определяют, как манипулирование расчётом затрат и выгод от действий противника. Уменьшая ожидаемые выгоды или увеличивая потенциальные издержки (или и то, и другое), можно убедить противника воздержаться от каких-то действий.⁵

Есть две основные формы сдерживания. Первая – *сдерживание путём недопущения*. Гленн Снайдер определил его как сдерживание за счёт возможности лишить другую сторону каких-то выгод от сдерживаемого действия.⁶ Майкл Мазарр показывает, что сдерживание путём недопущения основано на способности не допустить, эквивалентной способности защитить, и эффективно предотвращает действия, убеждая потенциального агрессора

³ Paul Kecskemeti, *Strategic Surrender: The Politics of Victory and Defeat* (Stanford, CA: Stanford University Press, 1958), 245-253.

⁴ Fiveable Content Team, “Deterrence,” *Fiveable: International Relations*, last updated August 2025, <https://fiveable.me/key-terms/introduction-international-relations/deterrence>.

⁵ Freedman, *Deterrence*.

⁶ Dmitry Adamsky, “Deterrence à la Ruse: Its Uniqueness, Sources and Implications”, в *NL ARMS Netherlands Annual Review of Military Studies 2020*, ed. Frans Osinga, Tim Sweijts (The Hague: T.M.C. Asser Press, 2021), 161-175, https://doi.org/10.1007/978-94-6265-419-8_9.

в том, что его действия невозможны и вряд ли увенчаются успехом, поэтому агрессор не может объективно надеяться на достижение своих целей.⁷ Вторая – *сдерживание путём наказания*, угрозы сурового возмездия (ядерной эскалации или разрушительных экономических санкций) в ответ на враждебный акт.⁸ Цель сдерживания посредством наказания заключается не в непосредственной защите ресурсов, а в угрозе общего наказания, что повысит цену нападения.

Определение сдерживания в России и в НАТО

Военная стратегия государства зависит от понимания и применения концепции сдерживания. Краткий сравнительный анализ понимания сдерживания в НАТО и в России позволяет объяснить оборонительную или наступательную позицию в военной стратегии этих игроков. Сдерживание может применяться не только в традиционной войне, но и в ответ на гибридные угрозы и нерегулярную войну.

Концепция сдерживания глубоко укоренилась в стратегии обороны государств и оборонительных альянсов, включая НАТО. НАТО рассматривает сдерживание и оборону, как основные задачи, и готова защищать свободу и безопасность всех союзников от всех угроз со всех направлений. Альянс препятствует агрессии, поддерживая эффективную стратегию сдерживания и обороны, сочетающую возможности ядерной, традиционной и противоракетной обороны, дополненные космическими и кибервозможностями.⁹ Российскую же стратегию сдерживания, напротив, можно охарактеризовать, как *действия до противодействия*. Книга Дмитрия Адамского «Сдерживание по-русски» содержит всесторонний анализ особого подхода России к сдерживанию, отмечая его важные отличия от западных парадигм.¹⁰

Как сдерживает Россия – важность диверсий

В российской стратегии термин «сдерживание» буквально означает «удержание», «недопущение», «отваживание». Он представляет собой многоуровневую стратегическую доктрину военной науки и геополитики.¹¹ В отличие от западного термина, с его акцентом на страхе, российский термин

⁷ Michael J. Mazarr, "Understanding Deterrence," *Perspective* no. 295 (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.

⁸ Mazarr, "Understanding Deterrence."

⁹ "Deterrence and Defence," NATO, December 10, 2025, www.nato.int/cps/en/natohq/topics_133127.htm.

¹⁰ Adamsky, "Deterrence à la Ruse: Its Uniqueness, Sources and Implications."

¹¹ Samuel Charap, "Strategic Sderzhivanie: Understanding Contemporary Russian Approaches to 'Deterrence,'" *Security Insights* No. 62 (Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies, September 2020), www.marshallcenter.org/en/publications/security-insights/strategic-sderzhivanie-understanding-contemporary-russian-approaches-deterrence-0.

лишён психологических коннотаций и сосредоточен на стратегическом наложении издержек.¹²

Военный энциклопедический словарь Министерства обороны определяет стратегическое сдерживание как согласованную систему мер несилового и силового характера, направленную на стабилизацию военно-политической обстановки, для сдерживания всех видов угроз с применением всех доступных государственных инструментов.¹³ В западном понимании стратегическое сдерживание перекликается с гибридной войной, принуждением в разных сферах и ядерным балансированием на грани войны.¹⁴ Для России безопасность предполагает постоянное давление на противников, включая НАТО и США.

Помимо *сдерживания*, важное место в российской доктрине занимает концепция *устрашения*. Она включает ядерные сигналы, открытые военные демонстрации, дезинформацию и психологические операции, направленные на дезориентацию и деморализацию противников.¹⁵ Эта логика проявилась в наращивании Россией военной мощи на границах Украины в 2021–2022 гг. для принуждения Запада к уступкам и удержания его от жёсткого ответа без прямого военного столкновения.

Диверсии, физические и кибернетические, являются одним из главных инструментов сдерживания в гибридном арсенале России. Министерство обороны США определяет диверсии как преднамеренное скрытое действие, направленное на повреждение, нарушение или выведение из строя критической инфраструктуры и ресурсов для достижения стратегических целей.¹⁶ Это соответствует как сдерживанию, так и устрашению, в соответствии с нацеленностью России на неопределённость и стратегическое принуждение.¹⁷ Этот асимметричный инструмент экономически эффективен, позволяет отрицать свою причастность и стратегически неоднозначен, размывая грань между миром и войной.¹⁸ Российские диверсии носят целенаправленный стратегический характер, наследуя советскую практику времён

¹² Charap, “Strategic Sderzhivanie.”

¹³ «Сдерживание стратегическое», Военный энциклопедический словарь, <https://1564.slovaronline.com/10093-сдерживание-стратегическое>.

¹⁴ Charap, “Strategic Sderzhivanie.”

¹⁵ Michael Kofman, Anya Loukianova Fink, “Escalation Management and Nuclear Employment in Russian Military Strategy,” *War on the Rocks*, June 23, 2020, <https://warontherocks.com/2020/06/escalation-management-and-nuclear-employment-in-russian-military-strategy/>.

¹⁶ “Exploring the Role of Covert Operations and Sabotage in Modern Military Strategies,” *Ops Defender*, May 8, 2024, <https://opsdefender.com/covert-operations-and-sabotage>.

¹⁷ Keir Giles, *Russia’s ‘New’ Tools for Confronting the West: Continuity and Innovation in Moscow’s Exercise of Power* (London: Chatham House, 2016), www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.

¹⁸ Валерий Герасимов, «Ценность науки в предвидении: Новые вызовы требуют переосмыслить формы и способы ведения боевых действий», *Военное обозрение*,

Холодной войны.¹⁹ КГБ и ГРУ были разработаны обширные планы тайных диверсионных операций против критической инфраструктуры Запада, которые должны были расколоть НАТО, деморализовать страны-участницы, нарушить цепочки поставок и посеять политические сомнения. Цели выбирали, исходя из их символического и стратегического значения: объекты энергетики (электростанции, нефтепроводы, НПЗ); транспорта (мосты, туннели, порты и автомагистрали); связи (телефонные узлы, радиолокационные станции). Диверсии планировались на ключевых экономических и военных объектах, включая порты Роттердама и Антверпена, использовавшиеся для тылового обеспечения во время войны во Вьетнаме, а также химические заводы и склады в Западной Германии. Велось наблюдение за западными силами спецназначения. Важными целями были пропагандистские центры, такие, как «Радио Свободная Европа» в Мюнхене, из-за их идеологической угрозы для советского блока.²⁰

Эта преемственность подтверждается доктриной Герасимова, с её стратегическим акцентом на невоенных инструментах. Диверсии поддерживают этот подход к гибридной войне, оставаясь ниже порога статьи 5 НАТО. По данным «Recorded Future», поджоги и самодельные взрывные устройства, а также использование подставных лиц, вербовка агентов, выбор целей и времени (на фоне поддержки Западом Украины) – характерные тактики, перекликающиеся с советской доктриной. Российская диверсионная деятельность опирается на методы, позволяющие отрицать свою причастность. Разведывательные сети вербуют агентов, способных проводить эти операции без прямого контакта с российским государством. Последние инциденты указывают на растущую роль подставных лиц, особенно иностранных граждан и преступников, завербованных для диверсий российской разведкой. Аресты по всей Европе выявили использование для атак балканских агентов, белорусских курьеров и местных информаторов без однозначного указания на причастность Москвы.²¹

В продолжение российских стратегий времён холодной войны, Европа столкнулась с резким ростом подобных актов после вторжения в Украину в 2022 году – возможно, самой масштабной волной, пережитой Западом после Второй мировой. Хотя официальные лица всё больше убеждаются в том, что многие из этих атак организует Кремль, отличительной чертой таких

январь-февраль 2016 (первоначально опубликовано в издании *Военно-промышленный курьер* 27 февраля 2013 года), https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html.

¹⁹ Daniela Richterova, “The Long Shadow of Soviet Sabotage Doctrine?” *War on the Rocks*, August 19, 2024, <https://warontherocks.com/2024/08/the-long-shadow-of-soviet-sabotage-doctrine/>.

²⁰ Richterova, “The Long Shadow of Soviet Sabotage Doctrine?”

²¹ Insikt Group, “Russian Sabotage Activities Escalate Amid Fraught Tensions,” Research Report, *Recorded Future*, November 14, 2024, <https://assets.recordedfuture.com/insikt-report-pdfs/2024/ta-ru-2024-1114.pdf>.

операций остаётся отрицание причастности. Разведывательные службы, западные правительства и лидеры НАТО публично осудили Россию и подтвердили, что диверсанты, арестованные в Польше, Германии, Румынии, Великобритании и Чехии, были связаны с российскими спецслужбами. Они также предупреждали об угрозе, исходящей от диверсантов, действующих на их территории по заданию России, хотя эти акты часто совершают не российские граждане, чтобы обеспечить Кремлю алиби. В странах ЕС и НАТО, занявших гибкую позицию по отношению к России или сохранивших нейтралитет (Венгрия, Турция, Австрия), не было диверсий в 2022–2025 гг., что может быть ещё одним доказательством её причастности.²²

Нынешнюю тактику российских диверсий можно разделить на три группы: экономические диверсии (удары по инфраструктуре, критичной для экономической стабильности), военные диверсии (нарушение производства вооружений, транспорта и боеготовности путём атак на оружейные заводы или центры материально-технического обеспечения), и политическая дестабилизация (усиление социально-политического раскола и устрашение местного населения посредством постоянной угрозы диверсий).²³ В докладе Хельсинкской комиссии США (2024 г.) указано, что Россия могла совершить около 150 диверсий (выглядевших как случайные инциденты) и других гибридных действий против стран НАТО, больше всего поддерживающих Украину, для достижения сразу нескольких целей: ослабления поддержки подвергнувшегося нападению государства, тестирования единства и стойкости НАТО, включая обязательства согласно статьям 4 и 5, вмешательства в национальные выборы в разных формах, выявления и повреждения критической инфраструктуры, а также ведения когнитивной войны посредством дезинформации и фейковых новостей для создания паники и подрыва доверия к правительствам и альянсам.²⁴ Эта тактика включала нарушение тылового обеспечения, поджоги, кибератаки, повреждение критических объектов энергетики и поддержку разного рода прокси. Нынешние операции нацелены на электросети, транспорт и общественную инфраструктуру, как и планировалось в советский период.

Масштаб и формы этих действий весьма разнообразны. Вот некоторые примеры: в Германии в октябре 2022 года были перерезаны важные железнодорожные кабели связи, что привело к остановке движения поездов на севере страны. В 2024 году был подожжён завод Diehl Metal, производящий зенитно-ракетные комплексы IRIS-T, и раскрыта связанная с Россией попытка убийства генерального директора Rheinmetall. Грузовой хаб DHL в Лейпциге был подожжён при помощи посылки, отправленной через Литву,

²² Insikt Group, “Russian Sabotage Activities Escalate Amid Fraught Tensions.”

²³ Insikt Group, “Russian Sabotage Activities Escalate Amid Fraught Tensions.”

²⁴ U.S. Commission on Security and Cooperation in Europe, *Spotlight on the Shadow War* (Washington, DC: U.S. Commission on Security and Cooperation in Europe, 2024), <https://www.csce.gov/wp-content/uploads/2024/12/Spotlight-on-the-Shadow-War-Website.pdf>.

в рамках более широкой транснациональной диверсионной сети. Не раз сталкивалась с инцидентами Польша, включая поджог лакокрасочного завода в январе 2024 года, масштабный пожар в главном торговом центре Варшавы в мае, а также арест нескольких иностранцев в связи с диверсиями. В Румынии гражданин Колумбии, подготовленный российскими агентами, был пойман при подготовке атак на объект инфраструктуры в Брагадиру в июле 2024 года, а во время президентских выборов страна столкнулась с более чем 85 000 кибератак и скоординированной дезинформацией. В Великобритании склад DHL в Бирмингеме подожгли при помощи посылки, вероятно, репетируя более масштабную диверсию, аналогично инциденту в Германии. В странах Балтии тоже было неспокойно: в конце 2024 года были повреждены подводные кабели между Финляндией и Эстонией, предположительно теневым флотом России, а также выведена из строя крупная линия электропередач Eastlink 2 – волочением по дну якоря. В июне 2024 года чешская разведка предотвратила попытку поджога автобусного депо в Праге, в мае в Литве в результате подозрительного пожара пострадал склад IKEA, а в 2023 году в Бельгии произошёл взрыв на складе военной техники в Антверпене.²⁵ В некоторых подвергшихся нападению странах ещё расследуют причины или устанавливают личности преступников, но Польша, Германия, Чехия, Дания, Великобритания и Румыния уже арестовали причастных к этим атакам. Однако операции часто начинаются через подставных лиц или российские сети в третьих странах, таких, как Беларусь, Сербия или даже страны Латинской Америки.²⁶ Правительства публично обвинили Россию, выразив уверенность в своих выводах.²⁷

²⁵ U.S. Commission on Security and Cooperation in Europe, *Spotlight on the Shadow War*.

²⁶ "NATO Says Russian Hybrid Attack Intensify on Members' Territories," *Reuters*, May 2, 2024, www.reuters.com/world/europe/nato-says-russian-hybrid-attack-intensify-members-territories-2024-05-02/; "Fake News from Russian, Belarusian Services Spiked during Floods in Poland, Minister Says," *Reuters*, September 25, 2024, www.reuters.com/world/europe/fake-news-russian-belarusian-services-spiked-during-floods-poland-minister-says-2024-09-25/; "From Russia to Serbia: How RT Spreads the Kremlin's Propaganda in the Balkans despite EU Sanctions," *Reporters Without Borders (RSF)*, September 30, 2024, <https://rsf.org/en/russia-serbia-how-rt-spreads-kremlin-s-propaganda-balkans-despite-eu-sanctions>.

²⁷ "Terrorist Group Responsible for Arson Attacks across Europe Taken to Court," *Eurojust – European Union Agency for Criminal Justice Cooperation*, 27 January 2026, <https://www.eurojust.europa.eu/news/terrorist-group-responsible-arson-attacks-across-europe-taken-court>; James C. Reynolds, "Russia Could Be Behind Cyber Attacks on British Businesses like M&S, NATO General Warns," *Independent*, December 4, 2025, www.independent.co.uk/news/world/europe/russia-cyber-attack-marks-and-spencer-nato-b2877844.html; Simon Lewis, "US Warns of Russian Effort to Tilt 2024 Elections in Europe against Ukraine," *Reuters*, January 18, 2024, www.reuters.com/world/us-warns-russian-effort-tilt-2024-elections-europe-against-ukraine-2024-01-18/; "Russian Hybrid Operations Very Concerning, Say Romania, Poland and Latvia," *Reuters*, June 11, 2024, www.reuters.com/world/europe/russian-hybrid-operations-very-concerning-say-romania-poland-latvia-2024-06-11/.

Учитывая сохраняющуюся геополитическую напряжённость, особенно затяжную войну на истощение и тупик в мирных переговорах, количество диверсий, вероятно, возрастёт, что говорит об острой необходимости эффективного сдерживания, предотвращения и пресечения подобных инцидентов.²⁸ Ожидается, что масштабы и изощрённость тайных операций будут расти, что, по всей видимости, является тревожным возрождением практики холодной войны в нынешних гибридных условиях.²⁹ Без надёжных контрмер эти тайные действия могут ослабить национальную безопасность и поддержку НАТО Украине. Для противодействия новой угрозе европейским странам необходимо активизировать обмен разведывательной информацией, защитить инфраструктуру и внимательно отслеживать потенциальные цели на предмет признаков эскалации.³⁰

Понимание стратегии диверсий времён Холодной войны в некоторой степени помогает нам предвидеть будущие диверсии и противодействовать им посредством сдерживания, предотвращения и локализации.

Подходы Запада/НАТО к сдерживанию и борьба с диверсиями

Западные представления о сдерживании основаны на недопущении, наказании и стойкости. Сдерживание по-русски эксплуатирует страх общества, слабости стратегической инфраструктуры, отрицание причастности и, возможно, самое важное – самоограничение противников, нерешительность в действиях из-за страха эскалации.³¹

В НАТО перешли от реагирования к более упреждающему и комплексному подходу к сдерживанию и защите от агрессии. Ключевым элементом этой трансформации стало принятие концепции сдерживания и защиты евроатлантического региона (Deterrence and Defense of the Euro-Atlantic Area, DDA), что стало существенным отходом от стратегии сдерживания НАТО после Холодной войны, ориентированной на урегулирование кризисов. Эта концепция изменила стратегическое планирование НАТО для решения проблем XXI века, особенно исходящих от всё более агрессивной России.³² Ковингтон подчёркивает, что этот новый подход к сдерживанию отражает по-

²⁸ “Countering Hybrid Threats,” NATO, updated January 29, 2026, https://www.nato.int/cps/en/natohq/topics_156338.htm; Insikt Group, “Russian Sabotage Activities Escalate Amid Fraught Tensions.”

²⁹ Eitvydas Bajarūnas, “The Hybrid Threat Imperative: Deterring Russia Before It Is Too Late,” Comprehensive Report (Washington, D.C.: Center for European Policy Analysis, 2025), <https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/>.

³⁰ Filip Bryjka, “NATO Members on Guard Against Russian Sabotage,” The Polish Institute of International Affairs (PISM), *Bulletin* No. 112 (2420), July 29, 2024, <https://pism.pl/publications/nato-members-on-guard-against-russian-sabotage>.

³¹ Adamsky, “Deterrence à la Ruse: Its Uniqueness, Sources and Implications.”

³² Stephen R. Covington, “NATO’s Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA),” Belfer Center for Science and International Affairs, Harvard Kennedy

нимание НАТО того, что нельзя ждать возникновения кризиса. Вместо этого эффективное сдерживание должно стать элементом повседневной деятельности Альянса уже в мирное время, постоянно демонстрируя военную готовность и комплексный подход, что демонстрирует меры и потенциал, лишая противника любых стратегических возможностей.³³

Важной особенностью концепции DDA является скоординированное применение наземных, воздушных, морских, кибернетических и космических возможностей. Это повышает способность НАТО реагировать на сложные гибридные угрозы, выходящие за рамки традиционного поля боя. Кроме того, DDA укрепляет политическое и военное единство НАТО, усиливая связь между стратегическим планированием и принятием политических решений. Ковингтон отмечает, что DDA повышает скорость и скоординированность реагирования в мирное, кризисное и военное время. Это важно не только для сдерживания агрессии, но и для управления эскалацией и удержания любого возможного конфликта под контролем. Эффективность DDA была продемонстрирована в ходе реагирования НАТО на вторжение России в Украину в 2022 году.³⁴ Это позволило быстро перебросить войска Альянса на восточный фланг, тем самым помешав России распространить конфликт за пределы Украины.

По словам Ковингтона, такая быстрая и скоординированная реакция протестировала DDA как инструмент управления кризисом и сдерживания войны.³⁵ Показав Москве, что Альянс силён и решителен, в НАТО реально повысили цену дальнейшей агрессии.³⁶ В целом, DDA стала концептуальной и оперативной основой новой, критически важной стратегической адаптации НАТО к реалиям современной войны и геополитического соперничества. Приняв упреждающий, комплексный подход к сдерживанию, НАТО укрепила коллективную оборону и продемонстрировала способность адаптироваться к новым вызовам в сфере безопасности.

Сдерживание диверсий – исключительно сложная задача

НАТО рассматривает диверсии как гибридную угрозу, которая может оставаться ниже порога обычного конфликта, что затрудняет определение виновных и реагирование. К ним относятся кибератаки, дезинформация, политическое вмешательство и тайные операции.³⁷ Диверсии – один из самых сложных и трудно реализуемых инструментов гибридной войны. Противодействовать им с помощью обычных мер сдерживания, предотвращения

School, August 2, 2023, www.belfercenter.org/publication/natos-concept-deterrence-and-defence-euro-atlantic-area-dda.

³³ Covington, "NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area."

³⁴ NATO, "Deterrence and Defence."

³⁵ Covington, "NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area."

³⁶ Covington, "NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area."

³⁷ NATO, "Countering Hybrid Threats."

или локализации нелегко, поскольку они сочетают черты обычной войны и терроризма. Диверсии объединяют военные, кибернетические, экономические и информационные тактики, применяемые скрытно, ниже порога открытого конфликта.

Сходство между диверсией и обычной войной заключается в их целях и последствиях. Обе они часто нацелены на стратегическую инфраструктуру – железные дороги, склады топлива, маршруты снабжения, – важные для оперативных возможностей противника, нарушение которых может вызвать панику.³⁸ Что касается последствий, то диверсии, как и обычная война, могут привести к немалым жертвам, включая ранения и гибель гражданского населения, например, в случае взрывов или поджогов. Иногда, если в результате инцидентов страдают граждане третьих стран, например, при таких международных инцидентах, как угон самолетов и взрывы, последствия диверсий могут выходить за рамки обычной войны.³⁹

Диверсии могут быть как самостоятельным инструментом гибридной войны, так и поддерживать военные операции. Однако, в отличие от обычной войны, диверсии могут осуществлять разведслужбы, группы сопротивления или наёмники. О них редко заявляют, и их трудно доказать, при отрицании причастности.⁴⁰

Цель и диверсий, и террора – влияние на процессы принятия военно-политических решений, а также на поведение общества, сея страх и неопределённость посредством разрушений и насилия. Их мишенью могут быть политические, экономические и военные объекты, повреждение которых приводит к беспорядкам, подрывает доверие общества и снижает оперативные возможности противника за счёт психологических эффектов страха и недоверия. Главное различие между ними заключается в том, что террор обычно нацелен на гражданское население, а диверсии – на инфраструктуру и физические или компьютерные сети, а не непосредственно на людей. Однако некоторые формы диверсий, такие, как поджог или нарушение электросетей, могут иметь те же последствия, что и терроризм.

Предотвращение диверсий – это не только недопущение ущерба стратегической инфраструктуре, но, что более важно, защита демократических институтов, экономической стабильности, боеготовности и политического

³⁸ Krzysztof Izak, "Terrorist and Sabotage Attacks on Selected Critical Infrastructure Systems – A Historical Perspective," *Terrorism – Studies, Analyses, Prevention*, Special Issue (2025): 71-111, <https://doi.org/10.4467/27204383TER.25.015.21518>.

³⁹ Witold Skomra, Karolina Wojtasik, "Critical Infrastructure as a Target for Hybrid Operations: Case Studies of Attacks Against the Facilities and Systems of CI," *Terrorism – Studies, Analyses, Prevention*, Special Issue (2025): 13-34, <https://doi.org/10.4467/27204383TER.25.013.21516>.

⁴⁰ Joshua Rovner, Rory Cormac, Lennart Maschmeyer, "Sand in the Gears: Sabotage in World Politics," *European Journal of International Security*, First View (2025), <https://doi.org/10.1017/eis.2025.10025>.

единства Альянса, а также серьёзное отношение к обязательствам коллективной обороны НАТО в условиях постоянных и растущих гибридных угроз. Поэтому предотвращать диверсии крайне важно, но и очень сложно, из-за их асимметричного характера. Надёжная стратегия сдерживания, полностью учитывающая реальные последствия, новые возможности поиска виновных и высокая стойкость могут сделать диверсии гораздо более дорогостоящими и менее привлекательными. В НАТО прямо заявили, что серьёзные гибридные атаки, включая диверсии, могут вылиться в применение статьи 5 о коллективной обороне.⁴¹ Это должно остудить противников, укрепляя коллективную оборону Альянса. Поскольку диверсии всё чаще рассматривают как главную тактику гибридной войны, особенно в свете враждебных действий России в евроатлантическом регионе, подход НАТО является частью общей стратегии обеспечения стойкости, сдерживания и защиты от нерегулярной войны.⁴² В НАТО публично осудили операции России в евроатлантическом регионе как враждебные и наметили план действий, включая расширение обмена разведданными, охрану критической и подводной инфраструктуры, усиление киберзащиты и слежку за российскими разведслужбами на территории стран-участниц.⁴³ В ответ на многочисленные диверсии НАТО и западные правительства активней принимают более решительные контрмеры.⁴⁴ В ряде стран НАТО созданы специальные группы для мониторинга и защиты критической инфраструктуры,⁴⁵ принимают новые стратегии национальной безопасности, правовую базу пересматривают и адаптируют к новым условиям безопасности.⁴⁶ В то же время правоохранительные органы тесно координируют действия с зарубежными партнёрами для расследования и предотвращения попыток диверсий.⁴⁷ Дальнейшие

⁴¹ NATO, "Deterrence and Defence."

⁴² NATO, "Deterrence and Defence."

⁴³ "Statement by the North Atlantic Council on Recent Russian Hybrid Activities," NATO, May 2, 2024, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/05/02/statement-by-the-north-atlantic-council-on-recent-russian-hybrid-activities>.

⁴⁴ "Resilience, Civil Preparedness and Article 3," NATO, updated November 13, 2024, <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>.

⁴⁵ "NATO's Maritime Activities," NATO, updated March 10, 2025, www.nato.int/en/what-we-do/operations-and-missions/natos-maritime-activities.

⁴⁶ "Critical Infrastructure Resilience at EU Level," European Commission, January 13, 2026, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.

⁴⁷ "Polish Army to Help Power Grid Protect Key Infrastructure," *Reuters*, December 3, 2025, www.reuters.com/business/aerospace-defense/polish-army-help-power-grid-protect-key-infrastructure-2025-12-03.

усилия также направлены на повышение стойкости общества за счёт повышения бдительности и осведомлённости граждан.⁴⁸

Ввиду стратегической туманности диверсий, сдерживание должно стать комплексной гибридной стратегией, объединяющей дипломатические, информационные, военные, экономические, контртеррористические и правовые инструменты.⁴⁹ Комплексное сдерживание гибридных угроз, включая диверсии, должно сочетать боеготовность вооружённых сил, юридическое установление вины, стойкость общества и стратегическое прогнозирование. Смягчение гибридных угроз требует повышения стойкости гражданского и военного секторов, партнёрства государства и частного сектора в защите критической инфраструктуры, превентивных мер по противодействию дезинформации и ограничению её психологического и политического воздействия,⁵⁰ а также стратегической коммуникации для контроля паники в обществе, укрепления национального единства и демонстрации решимости.⁵¹ Единая информационная политика, своевременное установление виновных и трансграничная координация усиливают сдерживающий эффект.⁵²

Инструменты сдерживания для НАТО и Запада

Запад ограничен в выборе невоенных ответных мер, за исключением широких экономических и дипломатических санкций против Москвы, которые станут ещё менее опасными для России, если в США решат их отменить. Тем не менее меры НАТО по борьбе с диверсиями включают широкий спектр тактик. К ним относятся политические сигналы, демонстрирующие единство и решимость,⁵³ поддержание боеготовности вооружённых сил в ходе совместных операций и учений для демонстрации надёжной обороны, оперативное развертывание для охраны уязвимой инфраструктуры,⁵⁴ учения по урегулированию кризисных ситуаций со сценариями диверсий для проверки и совершенствования стратегий реагирования, регулярная оценка и обновление протоколов безопасности для защиты критической инфраструктуры от кибердиверсий, киберкриминалистические исследования для

⁴⁸ House of Commons, Defence Committee, "Oral Evidence: Defence in the Grey Zone, HC 50," UK Parliament Committees, April 23, 2024, <https://committees.parliament.uk/oralevidence/14668/html>.

⁴⁹ "Hybrid Threats: Hybrid Threats as a Concept," European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), accessed January 24, 2026, www.hybridcoe.fi/hybrid-threats/.

⁵⁰ "Deterrence and Resilience," Hybrid CoE, Thematic reports and other publications (2023/2024), <https://www.hybridcoe.fi/deterrence-and-resilience/>.

⁵¹ "NATO's Approach to Counter Information Threats," NATO, updated February 3, 2025, https://www.nato.int/cps/en/natohq/topics_219728.htm.

⁵² NATO, "Countering Hybrid Threats."

⁵³ NATO, "Countering Hybrid Threats."

⁵⁴ NATO, "Countering Hybrid Threats."

разоблачения злоумышленников,⁵⁵ укрепление уязвимой инфраструктуры.⁵⁶ Стратегическая коммуникация для противодействия кампаниям дезинформации⁵⁷ и инициативы по повышению осведомленности населения тоже важны, поскольку они информируют частный и государственный сектора о рисках диверсий и поощряют сообщать о подозрительных действиях, что крайне важно для их своевременного выявления.

Другие меры, которые уже реализуются в ряде стран, но требуют развития или должны применяться как на национальном уровне, так и в рамках скоординированной стратегии союзников, включают:

- *Прогнозирование и предвидение тенденций диверсий*

Действенное сдерживание российских диверсий требует стратегического прогнозирования на основе выявления закономерностей, прецедентов и предвидения. В силу гибкого, скрытого и тайного характера диверсий их трудно предвидеть, особенно при действиях через агентуру, но распознавание и классификация устойчивых закономерностей в гибридной деятельности России служит хорошей отправной точкой для прогнозирования потенциальных целей и слабых мест и, соответственно, для выработки мер сдерживания и защиты.⁵⁸

Важно распознавать и прогнозировать угрозы на основе разведданных. Это включает составление карты потенциальных целей диверсий, таких, как объекты энергетики, транспортные узлы, системы связи и киберсистемы.⁵⁹ Их география, вероятно, будет включать Восточную Европу, страны Балтии, запад России, оккупированные территории Украины и гражданскую инфраструктуру НАТО.⁶⁰ Исходя из последних инцидентов, будущие диверсии могут включать кибератаки на инфраструктуру стран Северной Европы и Балтии, тайные атаки на железные дороги и центры логистики НАТО, перебои в энергоснабжении, гибридные операции с участием российских ЧВК на

⁵⁵ NATO, "NATO's Approach to Counter Information Threats."

⁵⁶ NATO, "NATO's Approach to Counter Information Threats."

⁵⁷ "NATO 2022 Strategic Concept Adopted by Heads of State and Government at the NATO Summit in Madrid," NATO, June 29, 2022, <https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf>.

⁵⁸ Hanna Mäkinen, "Russia's Hybrid Warfare in Europe," *Baltic Rim Economies*, no. 1 (January 2026): 141, https://www.centrumbalticum.org/files/7113/BRE_1_2026.pdf.

⁵⁹ Helmi Pillai, "Protecting Europe's Critical Infrastructure from Russian Hybrid Threats," Policy Brief, Centre for European Reform, April 25, 2023, www.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid.

⁶⁰ Anna Maria Dyer, "Preparing for Russian Hybrid Activities Against NATO and EU Countries," The Polish Institute of International Affairs (PISM), Bulletin No. 183 (2100), November 25, 2022, <https://www.pism.pl/publications/preparing-for-russian-hybrid-activities-against-natoand-eu-countries>.

Балканах, а также инциденты под чужим флагом, способные спровоцировать чрезмерную реакцию.⁶¹

Ключевые меры включают учёт уроков при моделировании угроз,⁶² инвестиции в прогнозирование, защиту объектов путём резервирования, усиление физической безопасности, выявление подозрительных действий в режиме реального времени и укрепление партнёрства государства с частным сектором, особенно в энергетике, транспорте и киберсекторе.

- *Поиск виновных*

В отличие от традиционной войны или терроризма, диверсии часто прячут под чужим флагом или негосударственными субъектами.⁶³ Поэтому сдерживание во многом опирается на достоверное расследование прошлых событий, за которым следуют правовые и экономические последствия, а также эффективное раннее предупреждение и сотрудничество в рамках страны и на международном уровне. Официальное публичное установление факта диверсии тоже может служить сдерживающим фактором, поскольку государство демонстрирует способность выявлять, расследовать и реагировать на тайные операции, а это может спровоцировать дипломатический или коллективный ответ противнику.

- *Подготовка и готовность*

Тактика сдерживания НАТО также включает высокий уровень военной готовности и присутствия, особенно в Восточной Европе, в рамках инициативы по усилению передового присутствия. Силы специальных операций и разведки развёртываются для мониторинга и обеспечения безопасности объектов повышенного риска.⁶⁴

Для лучшей готовности и обучения важно проводить регулярные учения со сценариями диверсий и кибератак, участвовать в многосторонних учениях НАТО по совместной защите инфраструктуры, а также развивать межотраслевую координацию и создавать межведомственные целевые группы. Учения и совместные операции вселяют уверенность в союзников и служат фактором сдерживания организуемых государством диверсий.

- *Стойкость*

НАТО призывает страны-участницы повышать стойкость, считая, что первая линия защиты от диверсий пролегает на национальном уровне. Альянс раз-

⁶¹ Seth G. Jones, "Russia's Shadow War Against the West," CSIS Briefs, Center for Strategic and International Studies, March 18, 2025, <https://www.csis.org/analysis/russias-shadow-war-against-west>.

⁶² Pillai, "Protecting Europe's Critical Infrastructure from Russian Hybrid Threats."

⁶³ Alex P. Schmid, "Defining Terrorism," ICCT Report, International Centre for Counter-Terrorism, March 2023, <https://icct.nl/publication/defining-terrorism>.

⁶⁴ "Strengthening NATO's Eastern Flank," NATO, October 23, 2025, www.nato.int/cps/en/natohq/topics_136388.htm.

работал базовые показатели стойкости ключевых секторов, поощряет регулярные стресс-тесты и доводит указания по гражданской готовности.

Тотальное сдерживание предполагает повышение стойкости и быстрое реагирование для повышения издержек для противника. Показательными примерами тут служат Эстония и Израиль.⁶⁵ Эстония внедрила систему быстрой идентификации и рабочие программы киберстойкости для государственного и частного сектора, разместила в Таллинне Центр передового опыта киберобороны НАТО (CCDCOE), усилила инфраструктуру и готова к сдерживанию.⁶⁶ Израиль делает акцент на упреждающем сборе данных, защите инфраструктуры, быстром ответном ударе и немедленном реагировании.⁶⁷ Страны Балтии диверсифицировали источники энергии, укрепили сотрудничество и воспользовались военной помощью НАТО и ЕС.⁶⁸ Стойкость и быстрое восстановление зависят от специальных кризисных групп (ремонт мобильных устройств и киберкриминалистика), партнёрства государства и частного сектора в области готовности и обмена информацией, а также создания дублирующих цепочек поставок и резервных систем, включая альтернативные каналы электропитания и связи.⁶⁹

- *Правовой ответ*

Эти оперативные шаги опираются на организационно-правовые меры. Гибридные угрозы требуют изменений права, особенно в отношении диверсий, схожих с тактикой террора – они должны быть поставлены вне закона. Усиление законодательных мер борьбы с терроризмом нужно распространить и на тайные диверсии, с суровым наказанием и ускоренными процедурами расследования для сдерживания посредством немедленного возмездия.⁷⁰ Многие страны НАТО усилили возможности контрразведки и приняли или обновили законы, направленные на борьбу с диверсиями, шпио-

⁶⁵ Peter W. Singer, Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014).

⁶⁶ Alexander Klimburg, ed., *National Cyber Security Framework Manual* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), <https://ccdcOE.org/library/publications/national-cyber-security-framework-manual>.

⁶⁷ Alon Ben-Meir, "Israel's Pre-Emptive Strategy and Peace," *AlonBen-Meir.com*, February 11, 1989, accessed January 24, 2026, <https://alonben-meir.com/writing/israels-pre-emptive-strategy-and-peace/>.

⁶⁸ "NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security," *News Release*, NATO, January 14, 2025, www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security.

⁶⁹ "The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Cyber Defence Hub," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), accessed January 24, 2026, <https://www.ccdcoe.org>.

⁷⁰ NATO, "Countering terrorism," What We Do, updated August 6, 2025, www.nato.int/en/what-we-do/deterrence-and-defence/countering-terrorism.

нажем и тайными операциями влияния. Лучшая координация военной полиции с гражданскими правоохранительными органами также укрепляет национальные системы безопасности.⁷¹

- *Кибербезопасность*

Кибербезопасность играет важную роль в предотвращении диверсий. Кибератаки уже признаны основанием для применения статьи 5 НАТО о коллективной обороне. Альянс создал группу быстрого реагирования на киберугрозы и сотрудничает с Евросоюзом и частным сектором для повышения киберстойкости своих членов. Гибридными угрозами, сочетающими кибероперации, дезинформацию и физические диверсии, занимается Центр передового опыта НАТО по противодействию гибридным угрозам в Финляндии, который поддерживает разработку индивидуальных стратегий и передовых методов.⁷² Кроме того, многие страны НАТО вкладывают значительные средства в инициативы кибербезопасности для защиты критической инфраструктуры от кибердиверсий, проводя регулярные оценки и обновляя протоколы безопасности.

- *Объединение стратегий борьбы с терроризмом*

Диверсии имеют ряд общих черт с терроризмом, включая использование небольших подпольных групп, символическую инфраструктуру в качестве целей, самодельные взрывные устройства в качестве инструментов, а также поджоги, кибервзлом и угрозы инсайдеров в качестве методов. Эффективное сдерживание и предотвращение диверсий, подобно контртеррористическим операциям, требуют многоуровневой стратегии, сочетающей разведку, координацию между гражданскими и военными, дублирование и физическую защиту инфраструктуры, правовые меры и возможности быстрого реагирования.⁷³

Методы, обычно используемые для снижения риска террористических актов, могут быть применены и для противодействия угрозе диверсий, особенно таких простых и эффективных, как поджог. Благодаря своей простоте, сложности доказывания и потенциальным катастрофическим последствиям, поджог стал излюбленным методом диверсий.⁷⁴ Для него требуется минимум ресурсов, не нужны передовые технологии и редко остаются

⁷¹ European Centre of Excellence for Countering Hybrid Threats, *Annual Report 2023*.

⁷² European Centre of Excellence for Countering Hybrid Threats, *Annual Report 2022*.

⁷³ United Nations Office of Counter-Terrorism and Counter-Terrorism Committee Executive Directorate, *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices* (New York: United Nations, 2018), www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf.

⁷⁴ Robert Arthur Baird, "Pyro-Terrorism – The Threat of Arson-Induced Forest Fires as a Future Terrorist Weapon of Mass Destruction," *Studies in Conflict & Terrorism* 29, no. 5 (2006): 415-428, <https://doi.org/10.1080/10576100600698477>.

следы для криминалистической экспертизы, что затрудняет выяснение точной причины пожара. Пожар может вызвать массовую панику и даже человеческие жертвы, нанося ущерб критической инфраструктуре далеко за пределами первичной зоны поражения и нарушая работу служб.⁷⁵

Чаще всего поджигают военные склады, транспортные узлы (для нарушения логистики), объекты энергетики (для отключения электроэнергии или создания дефицита топлива) и промышленные объекты (для остановки производства и нанесения экономического ущерба). В гибридной войне поджог часто используют наряду с кибератаками или дезинформационными кампаниями, тем самым увеличивая психологический и экономический ущерб.

Борьба с диверсиями в виде поджога требует особых мер. Значительно сократить время реагирования могут системы пожарной сигнализации, включая датчики дыма и тепла в сочетании с видеонаблюдением. Такие средства наблюдения, как дроны и тепловизоры, помогают выявлять подозрительную активность в критических зонах, а меры физической безопасности, включая ограждения и контроль доступа, позволяют предотвратить не санкционированное проникновение. В условиях ограниченного контроля государства, привлечение местных сотрудников и жителей к участию в программах общественного наблюдения обеспечивает дополнительный уровень бдительности.⁷⁶ Строгое соблюдение закона и судебное преследование поджигателей предотвращают возможные инциденты, а готовность к чрезвычайным ситуациям, включая противопожарные тренировки и группы быстрого реагирования, помогает ограничить ущерб.⁷⁷

- *Физическая защита стратегической инфраструктуры*

Стратегическим приоритетом НАТО стала защита критической инфраструктуры – электросетей, трубопроводов, подводных кабелей, средств транспорта и связи, а также военных объектов. В связи с этим Альянс поощряет обмен разведывательной информацией между союзниками и партнёрами для заблаговременного выявления попыток диверсий; совместным учениям для отработки гибридных и диверсионных сценариев и повышения

⁷⁵ Organization for Security and Co-operation in Europe (OSCE), *Project PROTECT – Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks* (Vienna: OSCE Secretariat, Transnational Threats Department, October 2025), www.osce.org/sites/default/files/f/documents/e/6/597756_0.pdf.

⁷⁶ “Enhancing Community Safety Against Incendiary Fires: Prevention and Awareness,” Approved Group International (community patrols and vigilance), August 13, 2024, <https://approvedgroupinternational.com/enhancing-community-safety-against-incendiary-fires-prevention-and-awareness/>.

⁷⁷ National Protective Security Authority (UK), “Fire as an Act of Sabotage Guidance: Countering the Threat of Sabotage Operations to UK Interests and National Security,” last updated September 25, 2024, www.npsa.gov.uk/national-security-act/countering-threat-sabotage-operations-uk-interests-national-security/fire-act-sabotage-guidance.

возможностей реагирования; повышению осведомленности о морской обстановке, особенно в Северном и Балтийском морях; и координации действий с бизнесом в энергетике и телекоммуникациях.⁷⁸ Другие меры включают целенаправленное внедрение протоколов безопасности, использование датчиков движения, камер видеонаблюдения и тепловизоров, оснащение уязвимых объектов барьерами и ограждениями, а также патрулирование беспилотниками и дистанционное спутниковое наблюдение за критическими зонами. Необходим также массовый контроль доступа и проверка персонала.⁷⁹ Одновременно следует усилить киберзащиту, особенно для систем диспетчерского управления и сбора данных (SCADA) и промышленных систем управления (ICS), чтобы предотвратить отключение систем сигнализации и пожаротушения до физической атаки.⁸⁰

В феврале 2023 года в НАТО был создан Координационный центр по критической подводной инфраструктуре для координации усилий союзников и повышения устойчивости базовой морской инфраструктуры.⁸¹ Кроме того, предлагаемая целевая группа ЕС-НАТО по устойчивости критической инфраструктуры должна формализовать обмен знаниями и координацию в этой области.⁸²

- *Информирование населения и гражданская готовность*

Для заблаговременного выявления угроз важны информационные кампании, направленные на информирование государственного и частного секторов о рисках диверсий и важности оповещения о подозрительной деятельности. Некоторые страны НАТО, в частности, Швеция и Финляндия, приняли подход «тотальной обороны», активно вовлекая население в планирование защиты страны и реагирование на кризисы.⁸³

- *Политика в отношении информаторов*

Участие населения и сбор информации на местах становятся первой линией защиты от саботажа. Укрепление доверия на местном уровне, поощрение

⁷⁸ NATO, “Resilience, Civil Preparedness and Article 3.”

⁷⁹ “NATO Allies Join Forces to Enhance the Security of Critical Undersea Infrastructure,” News, NATO, December 10, 2024, www.nato.int/en/news-and-events/articles/news/2024/12/10/nato-allies-join-forces-to-enhance-the-security-of-critical-undersea-infrastructure.

⁸⁰ Joshua Taylor, “Effectiveness of SCADA System Security Used Within Critical Infrastructure,” *ArXiv*, December 18, 2020, <https://arxiv.org/abs/2012.11375>.

⁸¹ “NATO Stands Up Undersea Infrastructure Coordination Cell,” News, NATO, February 15, 2023, https://www.nato.int/cps/en/natohq/news_211919.htm.

⁸² См. Табл. 1: “European Institutions Relevant for Protecting CUI” in Sean Monaghan et al., “NATO’s Role in Protecting Critical Undersea Infrastructure,” *CSIS Brief*, December 19, 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-12/231219_Monaghan_NATO_CUI.pdf.

⁸³ “Total Defence,” Government Offices of Sweden, accessed January 25, 2026, <https://www.government.se/government-policy/total-defence>.

информирования о подозрительной деятельности и умение населения сообщать о таких действиях позволяют властям создать агентурную сеть, способную выявлять ранние признаки подготовки диверсий. Это особенно важно в сельских или промышленных зонах с уязвимой критической инфраструктурой, где присутствие властей ограничено. Создание конфиденциальных механизмов для сотрудников, позволяющих сообщать о проблемах без страха ответных мер, также может способствовать повышению бдительности.

- *Расширение сотрудничества в сфере обороны и контрразведки*

Важным столпом стратегии сдерживания является расширение сотрудничества в области разведки и обороны. НАТО существенно улучшило обмен разведданными в режиме реального времени, сосредоточив внимание на иностранных разведслужбах и их агентуре, а также на внутренних угрозах со стороны местных противников и на оперативном планировании в странах-участницах для выявления, оценки и предотвращения диверсий. Обмен информацией о ситуации позволяет оперативно реагировать и координировать превентивные меры.⁸⁴ Стратегическое партнёрство и сотрудничество с партнёрами, не входящими в НАТО, и международными организациями способствуют обмену передовым опытом предотвращения диверсий и обеспечения коллективной безопасности. НАТО и союзники могут создать надёжную архитектуру сдерживания и противостоять современным угрозам диверсий посредством заблаговременного прогнозирования, обмена разведывательной информацией, защиты инфраструктуры и повышения стойкости общества.⁸⁵

- *Усиление возможностей быстрого реагирования*

Планирование противодиверсионных мер должно включать специализированные группы быстрого реагирования, обученные тушению пожаров, оценке ущерба и разрешению кризисных ситуаций. Эти группы должны тесно сотрудничать с правоохранительными органами и частными охранными компаниями для быстрого совместного реагирования. Противопожарные учения, планы эвакуации в чрезвычайных ситуациях и моделирование в режиме реального времени помогают повысить стойкость и готовность.⁸⁶

⁸⁴ NATO, "Resilience, Civil Preparedness and Article 3."

⁸⁵ Filip Bryjka, Tomasz Zając, "EU and NATO Countries Strengthen the Protection of Critical Infrastructure," Bulletin No. 79 (2198), PISM, June 22, 2023, www.pism.pl/publications/eu-and-nato-countries-strengthen-the-protection-of-critical-infrastructure.

⁸⁶ Lars Fredholm, Anna-Lena Göransson, eds., *Emergency Response Management in Today's Complex Society* (Swedish Civil Contingencies Agency, 2010); Luca Galbusera et al., "Game-based Training in Critical Infrastructure Protection and Resilience," *International Journal of Disaster Risk Reduction* 78 (August 2022): 103109, <https://doi.org/10.1016/j.ijdrr.2022.103109>.

Заключение

Стратегии сдерживания должны быть адаптированы к сложностям гибридной войны, особенно в условиях асимметричных угроз в «серой зоне», включая диверсии. Стратегическая эволюция НАТО в сторону упреждающего целостного подхода к сдерживанию, примером которого является концепция DDA, указывает на необходимость комплексной оперативной структуры для эффективного реагирования на эти угрозы.

Задача предотвращения диверсий, характеризующихся труднодоказуемостью и неопределённостью, требует комплексной стратегии, охватывающей правовые, экономические, военные, информационные и социальные аспекты. Защищая критическую инфраструктуру, информируя население и развивая международное сотрудничество, страны могут создать устойчивую систему сдерживания, способную противостоять прямым угрозам и обеспечить долгосрочную стабильность и безопасность. История показывает, что российская модель сдерживания применяется непрерывно как в мирное, так и в военное время; поэтому мы понимаем, что наша оборонительная стратегия тоже должна быть постоянной, ежедневной заботой, независимо от изменений в условиях безопасности. Уроки, извлечённые из прошлой и нынешней практики сдерживания, также будут иметь важное значение для выработки эффективного ответа на меняющуюся картину гибридных угроз.

Примечание

Мнения, выводы, заключения и рекомендации в данной публикации принадлежат автору и могут не отражать официальную политику или позицию Консорциума «Партнёрство ради мира», организаций-участниц и любых правительственных или международных организаций, связанных с его руководящими структурами.

Об авторе

Анка Анеску – выпускница Европейского центра исследований в области безопасности им. Дж. Маршалла, румынский политолог, специалист по геополитике Восточной Европы, нерегулярной войне и гибридным угрозам, особенно когнитивной войне и использованию взаимозависимостей в качестве оружия. <https://orcid.org/0009-0009-1690-5692>

Библиография

- “Salzburger Bierfleisch’ and the Legend of the Bull Washers,” *Salzburg.info*, https://www.salzburg.info/en/magazin/art-culture/salzburger-bierfleisch-and-the-legend-of-the-bull-washers_a_445970.
- “Countering Hybrid Threats,” NATO, updated January 29, 2026, www.nato.int/cps/en/natohq/topics_156338.htm.
- “Critical Infrastructure Resilience at EU Level,” **European Commission**, January 13, 2026, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terror-ism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.
- “Deterrence and Defence,” NATO, December 10, 2025, www.nato.int/cps/en/natohq/topics_133127.htm.
- “Deterrence and Resilience,” Hybrid CoE, Thematic reports and other publications (2023/2024), <https://www.hybridcoe.fi/deterrence-and-resilience/>.
- “*Enhancing Community Safety Against Incendiary Fires: Prevention and Awareness*,” Approved Group International (community patrols and vigilance), August 13, 2024, <https://approvedgroupinternational.com/enhancing-community-safety-against-incendiary-fires-prevention-and-awareness/>.
- “Exploring the Role of Covert Operations and Sabotage in Modern Military Strategies,” *Ops Defender*, May 8, 2024, <https://opsdefender.com/covert-operations-and-sabotage>.
- “Fake News from Russian, Belarusian Services Spiked during Floods in Poland, Minister Says,” *Reuters*, September 25, 2024, www.reuters.com/world/europe/fake-news-russian-belarusian-services-spiked-during-floods-poland-minister-says-2024-09-25/.
- “From Russia to Serbia: How RT Spreads the Kremlin’s Propaganda in the Balkans despite EU Sanctions,” Reporters Without Borders (RSF), September 30, 2024, <https://rsf.org/en/russia-serbia-how-rt-spreads-kremlin-s-propaganda-balkans-despite-eu-sanctions>.
- “Hybrid Threats: Hybrid Threats as a Concept,” European Centre of Excellence for Countering Hybrid Threats (**Hybrid CoE**), accessed January 24, 2026, <https://www.hybridcoe.fi/hybrid-threats/>.
- “NATO 2022 Strategic Concept Adopted by Heads of State and Government at the NATO Summit in Madrid,” NATO, June 29, 2022, <https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf>.
- “NATO Allies Join Forces to Enhance the Security of Critical Undersea Infrastructure,” News, NATO, December 10, 2024, <https://www.nato.int/en/news-and-events/articles/news/2024/12/10/nato-allies-join-forces-to-enhance-the-security-of-critical-undersea-infrastructure>.

- "NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security," *News Release*, NATO, January 14, 2025, <https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security>.
- "NATO Says Russian Hybrid Attack Intensify on Members' Territories," *Reuters*, May 2, 2024, <https://www.reuters.com/world/europe/nato-says-russian-hybrid-attack-intensify-members-territories-2024-05-02/>.
- "NATO Stands Up Undersea Infrastructure Coordination Cell," *News*, NATO, February 15, 2023, https://www.nato.int/cps/en/natohq/news_211919.htm.
- "NATO's Approach to Counter Information Threats," NATO, updated February 3, 2025, https://www.nato.int/cps/en/natohq/topics_219728.htm.
- "NATO's Maritime Activities," NATO, updated March 10, 2025, www.nato.int/en/what-we-do/operations-and-missions/natos-maritime-activities.
- "Polish Army to Help Power Grid Protect Key Infrastructure," *Reuters*, December 3, 2025, <https://www.reuters.com/business/aerospace-defense/polish-army-help-power-grid-protect-key-infrastructure-2025-12-03>.
- "Resilience, Civil Preparedness and Article 3," NATO, updated November 13, 2024, <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>.
- "Russian Hybrid Operations Very Concerning, Say Romania, Poland and Latvia," *Reuters*, June 11, 2024, <https://www.reuters.com/world/europe/russian-hybrid-operations-very-concerning-say-romania-poland-latvia-2024-06-11/>.
- "Сдерживание Стратегическое," *Military-Encyclopedic Dictionary Online*, n.d., accessed January 23, 2026, <https://1564.slovaronline.com/10093-сдерживание-стратегическое>. – in Russian
- "Statement by the North Atlantic Council on Recent Russian Hybrid Activities," NATO, May 2, 2024, www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/05/02/statement-by-the-north-atlantic-council-on-recent-russian-hybrid-activities.
- "Strengthening NATO's Eastern Flank," NATO, October 23, 2025, www.nato.int/cps/en/natohq/topics_136388.htm.
- "Terrorist Group Responsible for Arson Attacks across Europe Taken to Court," Eurojust – European Union Agency for Criminal Justice Cooperation, 27 January 2026, <https://www.eurojust.europa.eu/news/terrorist-group-responsible-arson-attacks-across-europe-taken-court>.
- "The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Cyber Defence Hub," *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, accessed January 24, 2026, <https://www.ccdcoe.org>.

- "Total Defence," Government Offices of Sweden, accessed January 25, 2026, <https://www.government.se/government-policy/total-defence>.
- Adamsky, Dmitry, "Deterrence à la Ruse: Its Uniqueness, Sources and Implications," in *NL ARMS Netherlands Annual Review of Military Studies 2020*, ed. Frans Osinga and Tim Sweijts (The Hague: T.M.C. Asser Press, 2021), 161-175, https://doi.org/10.1007/978-94-6265-419-8_9.
- Baird, Robert Arthur, "Pyro-Terrorism – The Threat of Arson-Induced Forest Fires as a Future Terrorist Weapon of Mass Destruction," *Studies in Conflict & Terrorism* 29, no. 5 (2006): 415-428, <https://doi.org/10.1080/10576100600698477>.
- Bajarūnas, Eitvydas, "The Hybrid Threat Imperative: Deterring Russia Before It Is Too Late," Comprehensive Report (Washington, D.C.: Center for European Policy Analysis, 2025), <https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/>.
- Ben-Meir, Alon, "Israel's Pre-Emptive Strategy and Peace," *AlonBen-Meir.com*, February 11, 1989, <https://alonben-meir.com/writing/israels-pre-emptive-strategy-and-peace/>.
- Bryjka, Filip, "NATO Members on Guard Against Russian Sabotage," *The Polish Institute of International Affairs (PISM), Bulletin* No. 112 (2420), July 29, 2024, <https://pism.pl/publications/nato-members-on-guard-against-russian-sabotage>.
- Bryjka, Filip, and Tomasz Zajac, "EU and NATO Countries Strengthen the Protection of Critical Infrastructure," *Bulletin* No. 79 (2198), PISM, June 22, 2023, <https://www.pism.pl/publications/eu-and-nato-countries-strengthen-the-protection-of-critical-infrastructure>.
- Charap, Samuel, "Strategic Sderzhivanie: Understanding Contemporary Russian Approaches to 'Deterrence'," *Security Insights* No. 62 (Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies, September 2020), <https://www.marshallcenter.org/en/publications/security-insights/strategic-sderzhivanie-understanding-contemporary-russian-approaches-deterrence-0>.
- Covington, Stephen R., "NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA)," Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2, 2023, www.belfercenter.org/publication/natos-concept-deterrence-and-defence-euro-atlantic-area-dda.
- Dyner, Anna Maria, "Preparing for Russian Hybrid Activities Against NATO and EU Countries," *Bulletin* No. 183 (2100), Polish Institute of International Affairs, November 25, 2022, <https://www.pism.pl/publications/preparing-for-russian-hybrid-activities-against-natoand-eu-countries>.
- European Centre of Excellence for Countering Hybrid Threats, *Annual Report 2023*.
- European Centre of Excellence for Countering Hybrid Threats, *Annual Report 2022*.

- Fiveable Content Team, "Deterrence," *Fiveable: International Relations*, last updated August 2025, <https://fiveable.me/key-terms/introduction-international-relations/deterrence>.
- Fredholm, Lars, and Anna-Lena Göransson, eds., *Emergency Response Management in Today's Complex Society* (Swedish Civil Contingencies Agency, 2010).
- Freedman, Lawrence, *Deterrence* (Cambridge, MA: Polity Press, 2004).
- Galbusera, Luca, et al., "Game-based Training in Critical Infrastructure Protection and Resilience," *International Journal of Disaster Risk Reduction* 78 (August 2022): 103109, <https://doi.org/10.1016/j.ijdr.2022.103109>.
- Gerasimov, Valery, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review* (January–February 2016): 23-29, www.armyupress.army.mil/Portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf.
- Giles, Keir, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power* (London: Chatham House, 2016), www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.
- House of Commons, Defence Committee, "Oral Evidence: Defence in the Grey Zone, HC 50," UK Parliament Committees, April 23, 2024, <https://committees.parliament.uk/oralevidence/14668/html>.
- Insikt Group, "Russian Sabotage Activities Escalate Amid Fraught Tensions," *Research Report, Recorded Future*, November 14, 2024, <https://assets.recordedfuture.com/insikt-report-pdfs/2024/ta-ru-2024-1114.pdf>.
- Izak, Krzysztof, "Terrorist and Sabotage Attacks on Selected Critical Infrastructure Systems – A Historical Perspective," *Terrorism – Studies, Analyses, Prevention*, Special Issue (2025): 71-111, <https://doi.org/10.4467/27204383TER.25.015.21518>.
- Jones, Seth G., "Russia's Shadow War Against the West," CSIS Briefs, Center for Strategic and International Studies, March 18, 2025, www.csis.org/analysis/russias-shadow-war-against-west.
- Kecskemeti, Paul, *Strategic Surrender: The Politics of Victory and Defeat* (Stanford, CA: Stanford University Press, 1958).
- Klimburg, Alexander, ed., *National Cyber Security Framework Manual* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), <https://ccdcoe.org/library/publications/national-cyber-security-framework-manual>.
- Kofman, Michael, and Anya Loukianova Fink, "Escalation Management and Nuclear Employment in Russian Military Strategy," *War on the Rocks*, June 23, 2020, <https://warontherocks.com/2020/06/escalation-management-and-nuclear-employment-in-russian-military-strategy/>.

- Lewis, Simon, "US Warns of Russian Effort to Tilt 2024 Elections in Europe against Ukraine," *Reuters*, January 18, 2024, <https://www.reuters.com/world/us-warns-russian-effort-tilt-2024-elections-europe-against-ukraine-2024-01-18/>.
- Mäkinen, Hanna, "Russia's Hybrid Warfare in Europe," *Baltic Rim Economies*, no. 1 (January 2026): 141, www.centrumbalticum.org/files/7113/BRE_1_2026.pdf.
- Mazarr, Michael J., "Understanding Deterrence," *Perspective* no. 295 (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.
- Monaghan, Sean, et al., "NATO's Role in Protecting Critical Undersea Infrastructure," *CSIS Brief*, December 19, 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-12/231219_Monaghan_NATO_CUI.pdf.
- National Protective Security Authority (UK), "Fire as an Act of Sabotage Guidance: Countering the Threat of Sabotage Operations to UK Interests and National Security," last updated September 25, 2024, <https://www.npsa.gov.uk/national-security-act/countering-threat-sabotage-operations-uk-interests-national-security/fire-act-sabotage-guidance>.
- NATO, "Countering terrorism," What We Do, updated August 6, 2025, www.nato.int/en/what-we-do/deterrence-and-defence/countering-terrorism.
- Organization for Security and Co-operation in Europe (OSCE), *Project PROTECT – Technical Guide on Physical Security Considerations for Protecting Critical Infrastructure from Terrorist Attacks* (Vienna: OSCE Secretariat, Transnational Threats Department, October 2025), www.osce.org/sites/default/files/f/documents/e/6/597756_0.pdf.
- Pillai, Helmi, "Protecting Europe's Critical Infrastructure from Russian Hybrid Threats," *Policy Brief*, Centre for European Reform, April 25, 2023, www.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid.
- Reynolds, James C., "Russia Could Be Behind Cyber Attacks on British Businesses like M&S, NATO General Warns," *Independent*, December 4, 2025, www.independent.co.uk/news/world/europe/russia-cyber-attack-marks-and-spencer-nato-b2877844.html.
- Richterova, Daniela, "The Long Shadow of Soviet Sabotage Doctrine?" *War on the Rocks*, August 19, 2024, <https://warontherocks.com/2024/08/the-long-shadow-of-soviet-sabotage-doctrine/>.
- Rovner, Joshua, Rory Cormac, and Lennart Maschmeyer, "Sand in the Gears: Sabotage in World Politics," *European Journal of International Security*, first view (2025), <https://doi.org/10.1017/eis.2025.10025>.
- Schmid, Alex P., "Defining Terrorism," ICCT Report, International Centre for Counter-Terrorism, March 2023, <https://icct.nl/publication/defining-terrorism>.

Singer, Peter W., and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014).

Skomra, Witold, and Karolina Wojtasik, "Critical Infrastructure as a Target for Hybrid Operations: Case Studies of Attacks Against the Facilities and Systems of CI," *Terrorism – Studies, Analyses, Prevention*, Special Issue (2025): 13-34, <https://doi.org/10.4467/27204383TER.25.013.21516>.

Taylor, Joshua, "Effectiveness of SCADA System Security Used Within Critical Infrastructure," *ArXiv*, December 18, 2020, <https://arxiv.org/abs/2012.11375>.

U.S. Commission on Security and Cooperation in Europe, *Spotlight on the Shadow War* (Washington, DC: U.S. Commission on Security and Cooperation in Europe, 2024), www.csce.gov/wp-content/uploads/2024/12/Spotlight-on-the-Shadow-War-Website.pdf.

United Nations Office of Counter-Terrorism and Counter-Terrorism Committee Executive Directorate, *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices* (New York: United Nations, 2018), https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf.