# Транснациональная незаконная торговля оружием в контексте гибридной войны: угрозы безопасности и комплексные меры нейтрализации

**Мороз Владимир Алексеевич**
Аспирант, кафедра стратегических коммуникаций и государственного управления; Дипломатическая академия Министерства иностранных дел Российской Федерации» (ДА МИД России), morozvova2001@mail.ru.

В работе исследуется феномен транснациональной незаконной торговли оружием как инструментального элемента гибридных войн. Актуальность исследования обусловлена качественной трансформацией нелегальных оружейных рынков: от стихийного разграбления арсеналов к управляемым государственными и негосударственными акторами логистическим сетям, встроенным в легальные коммерческие потоки. Целью работы является идентификация системных угроз, возникающих при интеграции теневых оружейных поставок в стратегию гибридного противостояния, а также разработка комплекса мер нейтрализации, выходящих за пределы традиционного экспортного контроля. Методологическую базу составляют системный анализ структурных связей между криминальными сетями и разведывательными сообществами, сравнительно-правовой анализ международных режимов регулирования, а также метод кейс-стади, применённый к конфликтам последнего десятилетия. Результаты исследования демонстрируют, что ключевая угроза смещается из плоскости количества оружия в плоскость его качества и управляемости поставок: на чёрные рынки поступают высокоточные системы, переносные зенитные ракетные комплексы и ударные беспилотники, что нивелирует технологическое превосходство регулярных армий.

**Ключевые слова:** транснациональная преступность, незаконная торговля оружием, гибридная война, прокси-силы, контрабанда, даркнет, криптовалюты, экспортный контроль, международная безопасность, сетецентрические угрозы, блокчейн-прослеживаемость

**Введение**

Завершение периода «холодной войны» породило большие надежды на достижение прочного мира и стабильности. Однако окончание XX и начало XXI в. характеризуются высокой динамикой политических событий, возникновением новых очагов напряженности в различных регионах, слабой предсказуемостью развития ситуации в мире. Сегодня в современных международных отношениях транснациональная незаконная торговля оружием перестала быть периферийной проблемой криминалистики или таможенного контроля [1, с. 6]. В условиях тотальной гибридизации конфликтов нелегальные потоки вооружений трансформировались в один из наиболее эффективных и при этом трудно доказуемых инструментов стратегического воздействия [2, с. 25]. В свою очередь гибридная война, стирающая различия между состоянием мира и войны, между солдатом и гражданским лицом, между легальными поставками и контрабандой, создала идеальную экосистему для процветания теневых оружейных рынков. В связи с этим незаконная торговля оружием на сегодняшний день обслуживает не только классические криминальные синдикаты, но и вполне респектабельные правительства.

Угроза, исходящая от этого явления, носит комплексный характер: она размывает монополию государства на легитимное насилие, удлиняет временной горизонт конфликтов, делает их экономически самодостаточными и, самое главное, создаёт эффект бумеранга, когда оружие, произведённое для одной гибридной кампании, через цепочку перепродаж возвращается в метрополию, обслуживая уже внутренний терроризм [3, с. 378]. Актуальность темы продиктована не столько ростом объёмов изъятий нелегального оружия, сколько качественным изменением самого ассортимента: на чёрные рынки проникают не только автоматы Калашникова, но и переносные зенитные ракетные комплексы, противотанковые управляемые ракеты, ударные беспилотники и средства радиоэлектронной борьбы. Это означает, что негосударственные акторы и террористические группы получают потенциал, способный нейтрализовать техническое превосходство регулярных армий, что кардинально меняет баланс сил в любом региональном конфликте. Целью данной работы является комплексный анализ транснациональной незаконной торговли оружием именно как инструмента гибридной войны, выявление структурных связей между криминальными сетями и спецслужбами, а также формирование системы мер нейтрализации, выходящих за рамки традиционного эмбарго и усиления пограничного контроля.

**Методы исследования**

Методологическая база исследования строится на сочетании системного подхода, позволяющего рассматривать незаконную торговлю оружием не как изолированные преступные эпизоды, а как устойчивую сетевую структуру, встроенную в глобальные политические процессы, и сравнительно-правового анализа, направленного на оценку эффективности существующих международных режимов контроля, таких как Программа действий ООН по стрелковому оружию или Вассенаарские договорённости. Эмпирическую базу составили открытые отчёты Стокгольмского института исследований проблем мира, доклады

Управления ООН по наркотикам и преступности, материалы Интерпола и Европола, а также аналитические записки неправительственных организаций, отслеживающих маршруты контрабанды.

**Результаты исследования**

Современная незаконная торговля оружием в контексте гибридной войны прошла три этапа эволюции. Первый этап, приходящийся на конец двадцатого века, характеризовался доминированием «наследственных» арсеналов: основные потоки формировались за счёт разграбления государственных складов в зонах распада государственности, как это было в Сомали, Афганистане или странах бывшей Югославии [5, с. 15]. Второй этап, охватывающий период глобальной войны с терроризмом, ознаменовался так называемым эффектом обратного слива, когда оружие, поставляемое легально союзным правительствам и повстанческим группам, оказывалось на чёрном рынке благодаря коррупции или военным поражениям. Третий, современный этап, непосредственно связанный с гибридными войнами, представляет собой принципиально иную модель. Это уже не стихийный рынок, а управляемый процесс, где поставки вооружений прокси-силам планируются заранее, финансируются через офшорные компании, а транспортировка осуществляется под прикрытием гуманитарных конвоев или коммерческих грузоперевозок с поддельными документами.

Ключевым выводом является наличие устойчивой корреляции между эскалацией гибридных кампаний и резким увеличением предложения на теневых рынках специфических видов вооружений, характерных именно для армий государств-агрессоров. Так, например, появление в Мали или Центральноафриканской Республике боеприпасов и осколочных гранат, произведённых в странах Восточной Европы в течение последних двух лет, невозможно объяснить только активностью криминальных группировок, что указывает на целенаправленную деятельность спецслужб по диверсификации каналов поставок.

Исследование выявило, что важнейшей угрозой безопасности становится феномен «оружейного вампиризма», когда нерегулярные вооружённые формирования, получив современные образцы вооружений, быстро адаптируют их под свою тактику, а устаревшие, но всё ещё боеспособные образцы сбрасываются на коммерческий чёрный рынок. Это создаёт долгосрочный негативный эффект, так как даже после урегулирования конкретного конфликта оружие остаётся в регионе на десятилетия, формируя среду для перманентной преступности и терроризма.

Отдельно следует выделить угрозу, связанную с «цифровизацией» контрабанды. Сегодня всё чаще сделки инициируются через даркнет и криптовалютные платформы, а логистика использует коммерческие платформы для совместных перевозок, что делает практически невозможным физический досмотр всех грузов. Фактически, незаконная торговля оружием стала стресс-тестом для либеральной экономической модели, основанной на свободе торговли и минимизации таможенных барьеров, поскольку преступники используют именно эти преимущества для быстрого перемещения товаров через границы.

Цифровизация транснациональной незаконной торговли оружием представляет собой не просто смену инструментов коммуникации, а фундаментальную трансформацию самой структуры преступного бизнеса, делающую его практически неуязвимым для традиционных методов правоприменения. Если ещё пятнадцать лет назад контрабанда вооружений требовала личных встреч, проверок через доверенных лиц, наличных расчётов в офшорных зонах и физической передачи товара из рук в руки, то сегодня весь жизненный цикл сделки, от поиска покупателя до финальной доставки, может быть осуществлён без единого контакта между продавцом и заказчиком.

Даркнет, вопреки расхожему мнению, давно перестал быть убежищем одиночек-энтузиастов и мелких дилеров. На таких платформах, как Hydra до её ликвидации или RAMP, а также на многочисленных зеркалах и вновь возникающих площадках, сформировалась полноценная инфраструктура верифицированных продавцов. Система работает по принципу маркетплейса: продавец получает рейтинг, отзывы, гарантии эскроу-счетов в криптовалюте. Покупатель из любой точки мира заходит через браузер Tor, выбирает товар из каталога, где зачастую указаны не только автоматы или пистолеты, но и гранатомёты, переносные зенитные комплексы и даже заказные партии боеприпасов, и оплачивает покупку биткоинами или анонимными монетами. Администрация площадки выступает гарантом, удерживая средства до подтверждения получения груза. Это полностью исключает классическую оперативную вербовку: оперативник не может внедриться в среду, потому что среды как привычного физического сообщества не существует. Есть анонимные никнеймы, которые сегодня активны, а завтра меняют ключи шифрования.

Однако критически важным звеном, обеспечивающим жизнеспособность этой схемы, является не столько даркнет, сколько легальная коммерческая логистика [6]. Именно здесь происходит разрыв между высокотехнологичным заказом и физическим перемещением товара, и именно здесь преступники достигли наибольшего успеха в эксплуатации уязвимостей либеральной экономической модели. Международная контейнерная перевозка, обрабатывающая десятки миллионов стандартизированных сорокафутовых контейнеров ежегодно, построена на принципах доверия и минимизации барьеров. Груз отправляется от двери до двери, пересекая за время пути до десяти-пятнадцати юрисдикций.

Таможенные службы физически способны досмотреть не более двух-трёх процентов от общего объёма. Даже современные сканеры не всегда позволяют идентифицировать разобранные узлы оружия, упакованные в пластик и залитые герметиком, или замаскированные под промышленное оборудование. Схема выглядит следующим образом: оружейный дилер в Пакистане или на Балканах заказывает контейнер, например, с мебелью или сельскохозяйственной продукцией. Внутри этого легального груза, в специально оборудованной полости, размещается партия пистолетов или комплектующих. Все документы оформлены идеально: инвойс, упаковочный лист, сертификаты происхождения. Контейнер следует через порты Стамбула, Пирея или Роттердама. На каждом этапе досмотр носит выборочный характер, и вероятность того, что именно этот контейнер откроют, крайне мала. Но даже если его откроют, найти скрытую полость, не имея точных координат закладки или рентгеновского аппарата высокого разрешения, практически невозможно.

Ещё более сложная для обнаружения схема использует платформы каршеринга грузоперевозок, так называемые биржи логистики. Сервисы вроде Uber Freight или европейские аналоги позволяют перевозчикам с простаивающим транспортом брать заказы на доставку [7, с. 60]. Преступные группы создают подставные компании-однодневки, регистрируются на таких платформах, получают заказ на перевозку совершенно легального товара, например, стройматериалов, и в пути осуществляют перевалку оружия. Водитель фуры, законно нанятый через цифровую платформу, часто даже не подозревает, что в паллете с гипсокартоном находится тайник. Он едет по навигатору, передаёт груз на складе получателю, получает

оплату на счёт компании. Цепочка рвётся здесь же: компания-перевозчик ликвидируется через неделю, следов не остаётся. Правоохранители могут задержать фуру, но доказывать умысел конкретного водителя, не имеющего никакого отношения к преступному сговору, крайне сложно, а грузоотправитель уже не существует юридически.

Отдельный пласт цифровизации связан с так называемым «производством на заказ». Речь идёт не столько о поставках готовых заводских изделий, сколько о контрабанде компонентов и 3D-технологиях. Цифровая модель оружейного ствола, затвора или даже рамки пистолета может быть зашифрована, разбита на тысячи пакетов данных и передана через мессенджеры типа Signal или Wire. На принимающей стороне находится коммерческая компания, владеющая фрезерным станком с числовым программным управлением. Формально компания занимается производством запчастей для автомобилей. Получив чертёж, станок вытачивает деталь, которая ничем не отличается от заводской, а иногда и превосходит её по качеству, если используется авиационный алюминий или титан. Далее эти детали через ту же даркнет-сеть координируются с другими производителями затворов, рамок, магазинов и ударно-спусковых механизмов. Все компоненты свозятся в единую точку сборки, иногда на территории третьей страны, где происходит финальная комплектация. Весь процесс юридически легален до самого последнего момента, потому что по отдельности ствол, рамка и затвор во многих юрисдикциях не считаются оружием до момента полной сборки. Эта схема делает бессмысленными традиционные попытки перекрыть каналы производства, поскольку завод-изготовитель как единая точка отказа просто отсутствует.

Использование криптовалют в этой экосистеме решает проблему трансграничного движения капитала, веками сдерживавшую крупную контрабанду. Биткоин-транзакции, особенно с использованием миксеров и протоколов конфиденциальности, не оставляют банковских следов. Невозможно арестовать счёт, если нет самого счёта в традиционном понимании, а есть лишь набор цифровых ключей, которые владелец может держать в голове. Даже когда правоохранителям удаётся идентифицировать криптокошелёк, средства могут быть перемещены за секунды через десятки промежуточных адресов. Более того, внедрение смарт-контрактов позволяет автоматизировать расчёты без посредников. Покупатель и продавец загружают условия сделки в блокчейн: средства блокируются на смарт-контракте и автоматически перечисляются продавцу при получении подтверждения доставки от независимого оракула, например, от логистической компании, которая сама не подозревает о своей роли в преступной схеме.

Таким образом, «цифровизация» контрабанды создала принципиально неустранимую асимметрию. Государство вынуждено защищать линейные границы — порты, аэропорты, почтовые терминалы. Преступник же атакует точечно и распределённо. Либеральная экономическая модель, основанная на свободе перемещения товаров, капиталов и услуг, минимизации бюрократических барьеров и уважении к коммерческой тайне, оказалась идеальной средой для масштабирования этого бизнеса. Каждое нововведение, призванное ускорить легальную торговлю — предварительное электронное декларирование, «единое окно», упрощённые таможенные коридоры, — неизбежно используется преступниками для легализации своих грузопотоков. Они не взламывают систему, они просто покупают билет в тот же поезд, что и законопослушные экспортёры, и едут с ними в одном вагоне. Единственный способ остановить этот процесс — не просто усиливать досмотр, что физически невозможно при текущих объёмах мировой торговли, а пересматривать саму парадигму доверия. Переход от выборочного контроля к тотальной цифровой прослеживаемости каждой единицы товара, внедрение систем сквозного мониторинга на основе блокчейна и искусственного интеллекта, анализирующего аномалии в логистических паттернах, — это неизбежная плата за сохранение безопасности. Однако такие меры вступают в прямое противоречие с интересами транснационального капитала, для которого любые дополнительные проверки означают рост издержек и замедление оборачиваемости. И пока это противоречие не разрешено, цифровая контрабанда оружия будет оставаться идеальным преступлением, идеально встроенным в механизмы глобальной экономики.

В ходе обсуждения полученных данных необходимо отойти от упрощённой трактовки проблемы как сугубо правоохранительной. Основное противоречие, которое делает незаконную торговлю оружием практически неискоренимой в краткосрочной перспективе, заключается в конфликте интересов между глобальным Севером и глобальным Югом. Развитые страны-производители вооружений формально заинтересованы в контроле, но негласно используют нелегальные каналы для решения своих геополитических задач, тогда как развивающиеся страны, сталкивающиеся с потоком контрабанды, не обладают ни техническими, ни финансовыми ресурсами для эффективного перехвата. Дискуссия вокруг введения глобальной системы маркировки оружия, включая нанесение меток на боеприпасы, уже более десятилетия блокируется именно из-за того, что прозрачность лишила бы государства возможности скрывать реальных получателей. Более того, система так называемых «конечных сертификатов пользователя», призванная гарантировать, что оружие не будет реэкспортировано третьей стороне, превратилась в фикцию. Исследование зафиксировало десятки случаев, когда правительства стран Прибалтики, Юго-Восточной Азии и Африки выдавали сертификаты на партии оружия, которое в течение двух недель оказывалось в распоряжении группировок, внесённых в террористические списки ООН.

Таким образом, ключевая проблема лежит не в плоскости технологий отслеживания, а в отсутствии политической воли и, что ещё важнее, в отсутствии механизмов принуждения, которые распространялись бы не на страны-транзитёры, а на непосредственных производителей. Представляется, что современная система санкций, ориентированная на эмбарго в отношении стран назначения, абсолютно неэффективна против гибридных схем.

Комплексные меры нейтрализации должны включать в себя, во-первых, переход от национальных систем контроля к наднациональной системе лицензирования производства, при которой любая партия оружия, независимо от заявленного конечного пользователя, должна фиксироваться в едином цифровом реестре с использованием технологий распределённого реестра. Это исключило бы возможность подмены документов. Во-вторых, необходима юридическая квалификация систематического снабжения негосударственных вооружённых групп на территории суверенного государства в качестве акта агрессии, что позволит применять к странам-спонсорам весь спектр мер коллективной самообороны. В-третьих, следует пересмотреть режим экспортного контроля в отношении продукции двойного назначения, поскольку именно компоненты для сборки беспилотников и систем связи стали сегодня основой «конструкторской» контрабанды. В-четвёртых, требуется создание специализированного трибунала или расширение мандата Международного уголовного суда для преследования высших должностных лиц, сознательно организующих каналы нелегальных поставок в

рамках гибридных войн. Параллельно должны развиваться программы обратного выкупа оружия и утилизации, но не как разовые акции, а как постоянный элемент постконфликтного урегулирования, финансируемый за счёт специального налога на транснациональные корпорации, работающие в оборонно-промышленном комплексе.

Формулируя выводы, необходимо подчеркнуть, что транснациональная незаконная торговля оружием в контексте гибридной войны является не столько криминальным бизнесом, сколько полноценным инструментом геополитического принуждения, делегитимизирующим классическое международное право. Угроза, исходящая от этого явления, уже сегодня достигла такого уровня, что способность государства контролировать свои границы и монополию на насилие поставлена под сомнение действиями не только террористов, но и вполне легитимных правительств других стран. Пока сохраняется разрыв между заявлениями о приверженности разоружению и реальными действиями по тайному вооружению прокси-сил, любые разговоры о построении стабильного миропорядка останутся декларацией. Оружие, попавшее в теневой оборот, приобретает свойство «чёрной дыры»: оно исчезает из официальной статистики, но продолжает работать, убивать и дестабилизировать на протяжении десятилетий. Нейтрализация этой угрозы невозможна без кардинального пересмотра отношения государств к суверенитету в вопросах производства и сбыта вооружений.

На сегодняшний день необходимо формирование глобального режима, при котором нелегальная торговля оружием будет рассматриваться не как правонарушение, а как преступление против мира и безопасности человечества, не имеющее срока давности. Только девальвировав оружие как доступный и эффективный инструмент политического влияния, отвязав его стоимость от способности радикально менять расстановку сил на поле боя, международное сообщество сможет перекрыть кислород гибридным войнам.

**Литература**


1. Бартош А.А. Законы и принципы гибридной войны. Военная мысль. 2022. № 10. С. 6-14.
2. Малышев А.Г., Абдуллина К.Р., Левин М.С. Проблема роста незаконного оборота оружия и пути ее разрешения в современных реалиях. В сборнике: Современные вопросы огневой подготовки и пути ее совершенствования. Сборник материалов научно-практического семинара с международным участием. Рязань, 2023. С. 25-29.
3. Поротов С.А., Шадчин И.Г. Незаконный оборот оружия: причины, последствия и пути решения проблемы. Аллея науки. 2024. Т. 1. № 9 (96). С. 378-381.
4. Balogun W. A. Dynamics of Illicit Arms Trade and Regional Security Challenges in West Africa: A Focus on Nigeria //Africa Review. – 2024. – Т. 17. – №. 1. – С. 1-21.
5. Mitrescu S., Sokolov M. In the Crosshairs: Hybrid Threats and the Challenge to Maritime //Defending Maritime Assets: Approaches to Critical Infrastructure Protection. – 2025. – С. 65.
6. Bertolini M., Minicozzi R., Sweijs T. Ten guidelines for dealing with hybrid threats: A policy response framework. – Hague Centre for Strategic Studies (HCSS), 2023.
7. Missiroli A. From hybrid warfare to'cybrid'threats-and back? Concepts, challenges, responses //Addressing Hybrid Threats. – Edward Elgar Publishing, 2024. – С. 40-56.


**Transnational Illegal Arms Trade in the Context of Hybrid Warfare: Security Threats and Comprehensive Countermeasures**


**Moroz V.A.**

The Diplomatic Academy of the Russian Ministry of Foreign Affairs.



This paper examines the phenomenon of transnational illicit arms trade as an instrumental element of hybrid warfare. The relevance of this study stems from the qualitative transformation of illicit arms markets: from the spontaneous looting of arsenals to logistics networks managed by state and non-state actors, integrated into legal commercial flows. The aim of this paper is to identify the systemic threats arising from the integration of illicit arms supplies into a hybrid warfare strategy, as well as to develop a set of countermeasures that go beyond traditional export controls. The methodological framework is based on a systemic analysis of the structural links between criminal networks and intelligence communities, a comparative legal analysis of international regulatory regimes, and a case study approach applied to conflicts of the last decade. The study's findings demonstrate that the key threat is shifting from weapons quantity to quality and supply chain management: high-precision systems, man-portable air defense systems, and attack drones are entering the black market, eroding the technological superiority of regular armies.



Keywords: transnational crime, illegal arms trade, hybrid warfare, proxy forces, smuggling, darknet, cryptocurrencies, export controls, international security, network-centric threats, blockchain traceability


**References**


1. Bartosh A.A. Laws and principles of hybrid warfare. Military Thought. 2022. No. 10. pp. 6-14.
2. Malyshev A.G., Abdullina K.R., Levin M.S. The Problem of Growing Illegal Arms Trafficking and Ways to Address It in Modern Realities. In: Current Issues in Firearms Training and Ways to Improve It. Collection of Materials from a Scientific and Practical Seminar with International Participation. Ryazan, 2023. pp. 25-29.
3. Porotov S.A., Shadchin I.G. Illegal Arms Trafficking: Causes, Consequences, and Solutions. Alley of Science. 2024. Vol. 1. No. 9 (96). pp. 378-381.
4. Balogun W.A. Dynamics of Illicit Arms Trade and Regional Security Challenges in West Africa: A Focus on Nigeria // Africa Review. - 2024. - Vol. 17. - No. 1. - pp. 1-21.
5. Mitrescu S., Sokolov M. In the Crosshairs: Hybrid Threats and the Challenge to Maritime //Defending Maritime Assets: Approaches to Critical Infrastructure Protection. – 2025. – P. 65.
6. Bertolini M., Minicozzi R., Sweijs T. Ten guidelines for dealing with hybrid threats: A policy response framework. – Hague Center for Strategic Studies (HCSS), 2023.
7. Missiroli A. From hybrid warfare to'cybrid'threats-and back? Concepts, challenges, responses //Addressing Hybrid Threats. – Edward Elgar Publishing, 2024. – pp. 40-56.