DOI: 10.17803/2542-2472.2025.33.1.019-026

СФЕРА СУВЕРЕННОГО ВИРТУАЛЬНО-ИНФОРМАЦИОННОГО НАЦИОНАЛЬНОГО ПРОСТРАНСТВА ГОСУДАРСТВА

Нестеров Анатолий Васильевич,
главный научный сотрудник Российского федерального центра судебной экспертизы,
доктор юридических наук, кандидат технических наук, профессор
109028, Россия, г. Москва, пер. Хохловский, д. 13/2
nesterav@yandex.ru

Аннотация. *Группа государств во главе с США фактически ведет гибридную войну, в которую входит составляющая «правовой войны». Поэтому в России необходима доктринальная основа для создания нормативных правовых актов и нормативно-технических документов, позволяющая обеспечить суверенитет в любой инцидентной ситуации, затрагивающей интересы России, в любом домене (локальном, территориальном и/или глобальном) сферы виртуально-информационного пространства. Вопросы суверенизации национального пространства стали важными и актуальными. Инциденты, возникающие в виртуально-информационном пространстве, метафорично называемом «цифровым», требуют наличия юрисдикционного механизма выявления (конкретизации) актора (источника, продуцента и/или продукта). В частности, применения судебной юрисдикции, в том числе экспертизы в юрисдикционных целях, позволяющих получать судебно-экспертные доказательства, и принимать судебные решения. Кроме того, в определенных ситуациях необходимо применять ответные меры, которые должны соответствовать установленным в национальном законодательстве нормам реагирования в ситуациях, возникающих в виртуально-информационном пространстве. В статье используются категорийно-тензорный и продуцентный подходы, разрабатываемые автором. Показана необходимость доктринального обсуждения категорий домена, пространства и ситуации в виртуально-информационном пространстве. Аргументировано, что национальный суверенитет должен распространяться не только на носителей в «киберпространстве», данные в пространстве данных, но и на содержимое (контент) знак-продуктов (знаков сведений, сигналов сообщений и/или кодов двоичных данных), несущих семиотическое содержание (информацию), идеи и/или формы, представляющие действительные и/или существующие сущности в виртуально-информационном пространстве, которые способны воздействовать на психосоциальные свойства населения.*

Ключевые слова: *доменные пространства; психосоциальное воздействие; принадлежность; коммуникативный; когнитивный; ментальный; содержимое; содержание; идеи.*

THE SPHERE OF SOVEREIGN VIRTUAL AND INFORMATION NATIONAL SPACE OF THE STATE

Anatoliy V. Nesterov,
Dr. Sci. (Law), Cand. Sci. (Technology), Professor, Chief Researcher, Russian Federal Center for Forensic Science, Moscow, Russian Federation
nesterav@yandex.ru

Abstract. *A group of states led by the United States is effectively conducting a hybrid war that contains such an element as «lawfare». Therefore, Russia needs a doctrinal foundation for making regulatory acts and normative-technical documents that ensure sovereignty in any incident situation affecting the interests of Russia in any domain (local, territorial, and/or global) of the virtual-informational space. The issues of sovereignizing the national space have become important and relevant. Incidents taking place in a so-called «digital» virtual-informational space require a jurisdictional mechanism for identifying (specifying) the actor (source, producer, and/or product), in particular, this involves the application of judicial jurisdiction, including expertise for jurisdictional purposes, which allows admission of judicial-expert evidence and making judicial decisions. Furthermore, in specific situations, it is necessary to apply countermeasures that must comply with the norms of response established in national legislation for situations arising in the virtual-informational space. The paper relies on categorical-tensor and producent approaches developed by the author. The paper demonstrates the need for doctrinal discussion of the categories of domain, space, and situation in the virtual-informational space. It is argued that national sovereignty should extend not only to carriers in «cyberspace» in the data space, but also to the content of sign-products (signs of information, signal messages, and/or binary data codes) that carry semiotic content (information), ideas, and/or forms representing real and/or existing entities in the virtual-informational space that can influence the psychosocial properties of the population.*

Keywords: *domain spaces, psychosocial impact, belonging, communicative, cognitive, mental, content, contents, ideas.*

Потенциальные противники Российской Федерации фактически развязали необъявленную прокси-войну, а «полем боя» стало все наше население, в том числе должностные лица в организационных структурах и/или органах публичной власти. От способов «мягкой силы» и «цветных революций» они перешли к способам психосоциального воздействия с помощью виртуально-информационных инструментов. Сейчас аналитики США и НАТО такие способы стали называть «когнитивно-ментальными».

Телеком-интернет-инфраструктура на основе радиоэлектронных носителей, несущих знак-продукты (медиа-продукты), применяется для психосоциального воздействия, что позволяет противнику атаковать психику людей на всей территории Российской Федерации. Целью атак становятся люди, имеющие телефон или доступ к социальной сети, мессенджеру, электронной почте, т.е. устройствам и знакоместам в виртуально-информационном пространстве. Также противник применяет все возможные инструменты по оказанию давления на Российской Федерации: политические по изоляции, экономические за счет применения рестрикций, юрисдикционные путем создания прецедентов, военные провокации для принуждения к ответным мерам, а также в культурной, спортивной жизни и т.д.

Наибольшего результата противник достигает в виртуально-информационном пространстве за счет имеющегося преимущества, что требует принятия адекватных норм в национальном законодательстве и применения юрисдикционных и фактических ответных мер. Сфера виртуально-информационного пространства

не имеет физических границ, а подписание международного договора, регулирующего правоотношения, деятельность и продукты в этом пространстве, тормозится группой стран во главе с США. Этим пользуются транснациональные медиа-корпорации, недружественные организационные структуры и отдельные лица, которые нарушают национальное законодательство Российской Федерации.

В нашей стране необходима доктринальная основа для создания нормативных правовых актов и нормативно-технических документов, позволяющая обеспечить суверенитет в любой инцидентной ситуации, затрагивающей интересы России, в любом домене (локальном, территориальном и/или глобальном) сферы виртуально-информационного пространства. Вопросы суверенизации национального пространства стали важными и актуальными[1].

Важной является национальная исполнительная и/или судебная юрисдикция с ее криминалистической и/или судебной экспертизой, позволяющей получать судебно-экспертные доказательства, обеспечивающие правоприменение. Виртуально-информационная безопасность Российской Федерации в психосоциальной подсфере человеческой сферы должна обеспечить неприкосновенность населения, организационных структур и/или органов публичной власти, как от внешних, так и внутренних попыток ее нарушить. При этом недопустимо некорректно копировать иностранные нормы или стандарты, а необходимо осуществить суверенизацию национальных норм и стандартов, т.к. метафоричность некоторых иностранных норм и стандартов, позволяет противнику применять их по своему усмотрению. Особенно это должно касаться ситуационного национального суверенитета.

В сфере глобального виртуально-информационного пространства появился новый домен противоборства между государствами. Поэтому представляется важным и актуальным попытаться ответить на следующие вопросы: кто (что), когда, где, как, почему и/или зачем является целью воздействий недружественных стран на Российскую Федерацию. На два последних вопроса можно ответить сразу, а остальные требую более подробного обсуждения. Судя по всему, у глобального капитализма появились территориальные ограничения на Земле, поэтому стали применяться колониальные способы разделения, ограничения, сдерживания, изоляции и т.д. других стран с богатыми ресурсами. На вопрос: почему возникла экспансия, есть вариант ответа: несоответствие своих потребностей, возможностей потреблять ресурсы и/или внешней допустимости получить доступ к ресурсам. На вопрос: зачем, — можно ответить так: устранение несоответствия за чужой счет, прикрываясь декларациями о демократии, свободе и/или правах человека.

В США и НАТО на смену идеологической борьбе пришли новые способы «мягкой силы» воздействия на население крупных государств и «цветных революций» малых стран. В последнее время появился новый домен (театр военных действий) в виде когнитивно-ментального домена, хотя известна дискуссия по этому поводу, в которой далее примем участие. Если по двум доменам: территориальному (суше, морю и воздуху) и глобальному (космическому пространству и пространству электромагнитного спектра) государства смогли договориться об их регулировании на международном уровне, то по виртуально-информационному пространству — нет.

США давно применяет способ привлечения высококвалифицированных иммигрантов («утечки мозгов» из других государств), т.к. колониальная политика базируется на высокотехнологичном превосходстве и сдерживании развития стран-конкурентов политическими, экономическими, социальными, технологическими и т.д. методами. Например, в информационно-коммуникационном пространстве, которое в США метафорично именуется «киберпространством», они имеют преимущество за счет транснациональных медиа-корпораций. Так как власть в США, банки и эти корпорации тесно сотрудничают, о независимости СМИ сложно говорить. Такие же связи имеются у США с государствами — членами НАТО. При этом США не стесняется

[1] *Румянцева В. Г.* Государственный интерес: власть суверена по умолчанию // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 11. С. 165–170.

говорить о своем глобальном доминировании в мире, игнорируя ООН, и придумывая «правила» для объявления глобальности их интересов в любой точке Земли.

Домен киберпространства подразумевает телеком-интернет-инфраструктуру на основе радиоэлектронных носителей, без учета того, что может распространяться в ней и вне зависимости от территориальных границ, т.е. то, что метафорично называется «информацией». Позиция США по поводу информации в киберпространстве демагогически определяется свободой слова, которая «несет» демократию и обеспечивает права человека. Однако в действительности, транснациональные медиа-корпорации со штаб-квартирами в США часто не соблюдают национальные законодательства государств и права граждан, что незаконно, и требует применения контрмер.

Информация в телеком-интернет-инфраструктуре стала оружием воздействия на когнитивные (познавательные) способности и/или ментальные (национальные, традиционные и/или культурные) свойства населения атакуемой страны. Аналитики США и НАТО перешли от идеологического противостояния в «холодной войне» к активным формам «гибридной войны» в виде психосоциальных воздействий на целевую массу людей для негативного манипулирования не только массовым сознанием целевого населения, но и подрыва их «традиционных корней» (менталитета).

«Полем» противодействия становится цивилизационное пространство многонационального, многоконфессионального и/или многокультурного государства, т.е. идентичность его граждан в принадлежностном пространстве. Это стало возможным благодаря появлению больших хранилищ мультимодальных двоичных данных, метафорично называемых «цифровыми». Кроме того, возникла очередная волна создания программно-управляемых систем, метафорично называемых «искусственным интеллектом» на основе «глубокого обучения», систем «блокчейн» и систем «метаверс». Все эти системы можно называть смарт-системами, которые могут автоматизировать рутинные умственные операции. Особенностью таких систем является продуцирование виртуально-информационного пространства, в котором пользователи и виртуальные сущности могут взаимодействовать между собой, как в виртуальном, так и действительном пространстве.

Для НАТО разрабатывается концепция когнитивно-ментального доменного пространства[2]. Особенностью когнитивно-ментальной войны является то, что ее невольными соучастниками могут стать обычные люди, у которых может измениться психосоциальное состояние. В отчете для НАТО[3] отмечено, что основной уязвимостью человека является его психика, поэтому необходимо воспользоваться этим. В этом отчете прямо говорится, что «цель когнитивной войны — нанести вред обществу, а не только военным». Фактически предлагается ввести еще одно доменное пространство, в котором единицей будет сознание как минимум одного человека и не обязательно военного. В публикации Е. Макарова приведен обзор и анализ мнений ученых по поводу метафор «когнитивная» и «ментальная» война и он приходит к выводу, что «Когнитивная война направлена на обман человеческого мозга путем выявления и эксплуатации ошибок восприятия и суждений отдельных индивидов, групп или больших сообществ — государств, наций. Средствами данного обмана является технически оформленная коммуникативная сфера межличностных взаимодействий... Ментальная война... строится путем обмана и манипуляций в сфере познавательной деятельности человека и замещения культурных

[2] *Norton B.* Behind NATO's «cognitive warfare»: «Battle for your brain» waged by Western militaries // Grayzone. 2021. № 8. URL: https://thegrayzone.com/2021/10/08/nato-cognitive-warfare-brain/ (дата обращения: 20.03.2025).

[3] *Cao K., Glaister S.* et al. Countering cognitive warfare: awareness and resilience // NATO Review. (20 May 2021). Johns Hopkins University & Imperial College London. URL: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html (дата обращения: 20.03.2025).

и социальных принципов сообщества»[4]. Идеолог когнитивной войны Ф. Клюзель считает: «Когнитивная война — это нетрадиционная форма ведения войны, которая использует кибернетические инструменты для изменения познавательных процессов противника; эксплуатирует предубеждения, рефлексивные влияния на принятие решений и препятствие действиям, провоцирующее негативные последствия как на индивидуальном, так и на коллективном уровне»[5]. В России под ментальной войной понимается борьба за мировоззрение, идентичность и идеологию с целью полной «оккупации» сознания противника, в то время как под когнитивной — методы и способы военных действий и боевых операций[6].

В 2022 г. под доменом в США стали понимать оперативную военную среду, в которой виды шести доменов изменились: вместо домена электромагнитного спектра появился ментальный домен когнитивного доминирования[7], а это говорит о том, что направление психологических операций сформировалось в виде когнитивно-ментальных операций. Таким образом, аналитики НАТО пока не определились с категорией домена в военном деле. Отметим, что эта категория должна быть универсальной и пригодной для всех предметных областей.

Виды доменов (доменных пространств) могут состоять как минимум из одной границы, отделяющей внутренние единицы окружения от внешних. Под единицей окружения понимается как минимум один гетероморфный (парный) и/или гомоморфный (похожий, но разный, тройственный) индивид и/или многоморфный, а также один изоморфный (одинаковый) элемент окружения.

Границы могут быть конкретными (внутренними и/или территориальными) и/или глобальными (неопределенными). Три вида доменов могут состоять из внутреннего окружения локальной ситуации и/или внешнего окружения (территориального домена и/или глобального домена). Границы доменов могут разделять материально-вещественные носители, в частности территориальные в виде суши, моря и/или воздуха, глобальные в вид космоса (безвоздушного пространства) и/или электромагнитного спектра (электромагнитного излучения и/или напряженности электромагнитного поля). На основе электронных носителей и радиочастотных носителей известны глобальные радиоэлектронные носители, на базе которых продуцируется домен техногенной сферы в виде телеком-интернет-инфраструктуры.

Кроме того, носители могут нести содержимое знак-продуктов (медиа-продуктов) в виде семиотического содержания, форм и/или идей. Поэтому можно говорить об элементах окружения для индивидов в виде знак-продуктов, например, для текста — это будет контекст.

Военная деятельность может осуществляться не только в доменах, как окружениях, но и в сферах (геосфере, биосфере и/или антропосфере) и/или в мирах (микромире, мезомире (наблюдаемом мире) и/или макромире. Основной сферой для вооруженных ситуаций являются человеческая, общественная и/или техногенная подсферы антропосферы. Техногенная подсфера включает в себя виртуально-информационную сферу, носителями единиц которой, являются радиоэлектронные носители, где радиочастотные носители основаны на волнах электромагнитного спектра.

---

[4] *Макаров Е.* Ментальная и когнитивная войны — вопросы определения, цели и средства // Геополитика.ru. URL: https://www.geopolitika.ru/article/mentalnaya-i-kognitivnaya-voyny-voprosy-opredeleniya-celi-i-sredstva?ysclid=m5k1d6czeq891503478 (дата обращения: 20.03.2025).

[5] *Claverie B., Cluzel F.* The Cognitive Warfare Concept // NATO Allied Command Transformation / Innovation Hub. 2021. URL: https://2050.su/the-cognitive-warfare-concept/?ysclid=m5kopvahv450540445 (дата обращения: 20.03.2025).

[6] *Ильницкий А. М.* Стратегия ментальной безопасности России // Военная мысль. 2022. № 4. С. 24–35.

[7] Air-Force General Eric Autellet, Dr. Norbou Buchler et al. Cognitive Warfare Symposium. ENSC // NATO Science and Technology Organization. 2021. URL: https://2050.su/cognitive-warfare-the-future-of-cognitive-dominance/?ysclid=m5kovrrhds752346147 (дата обращения: 20.03.2025).

Общественная сфера может состоять из политической, социальной, юридической и т.д. подсфер. Нас интересует социальная сфера, т.к. человек, кроме уникального тела, обладает уникальной психикой и/или уникальными социальными навыками. Единицей человеческой подсферы можно считать как минимум одну человеческую сущность в виде хотя бы одной величины по крайней мере одного телесного (электро-биохимического), личного (психического) и/или личностного (социального), а также политико-юридического (лицевого, гражданского) свойства, сущего и/или одной связи. Именно население становится целью психосоциальных атак (прямых, опосредованных через прокси и/или косвенных через окружение, а также с помощью инструментов, в частности телеком-интернет-инфраструктуры, в рамках которой продуцируется пространство знак-продуктов. На основе единиц виртуальных сущностей знак-продуктов (медиа-продуктов) продуцируется виртуально-информационное пространство, сущности которого могут оказывать психосоциальные воздействия на сознание и/или память как минимум одного человека и/или неявно минуя их, на всю психику, включая неосознаваемую составляющую, еще называемую «подсознанием».

К уязвимостям человека можно отнести его психосоциальную сущность на основе нервной ткани головного мозга, личную психику (сознание, память и/или неосознаваемые иррациональные, эмоциональные и/или творческие составляющие) и/или личностные социальные навыки. Отметим, что психосоциальная сущность человека (сущее, свойства и/или связи) достаточно устойчива, т.к. формируется в детстве и молодости. Однако современные психосоциальные способы воздействия на психику и/или социальное поведение молодого поколения позволяют качественно трансформировать его в нужную манипуляторам сторону, что подтверждается опытом такого воздействия на постсоветском пространстве.

Психосоциальное воздействие направлено на мышление (то, как человек мыслит), что не исключает необходимости воздействия на то, что он мыслит, а также почему и/или зачем он мыслит. Человек мыслит невидимыми идеями и умственно выражает их знаками, которые имеют форму и/или семиотическое содержание. Также важно, с помощью чего, осуществляется психосоциальные воздействия, в частности носители, знак-продукты и/или идея-продукты, и наконец, их содержание и/или форма.

Вне зависимости от носителя знак-продукта (медиа-продукта) в виде знаков сведений, сигналов сообщений и/или кодов двоичных данных, его содержимое имеет декларативный, инструктивный и/или мотивирующий характер. Именно, последнее может оказывать влияние на психосоциальную сущность неподготовленного пользователя, у которого не развито критическое мышление, позволяющее ему выявлять в содержимом знак-продукта подлинную, поддельную (ложную) и/или шумовую составляющие. Кроме того, он может быть осторожным и/или здравомыслящим, чтобы не стать участником распространения мизинформации (дезинформации, которая распространяется по недомыслию и/или неосторожности). Негативное психосоциальное содержание медиа-продуктов может носить мотивирующий характер и сопродуцировать в психосоциальной сущности пользователя коммуникативный продукт не только в его сознании, но и минуя его, в психике и/или социальном поведении. Это связано с тем, что такое содержимое может быть направлено на психосоциальные уязвимости и иметь скрытую составляющую, направленную на сопродуцирование психосоциальных расстройств, а также быть безсодержательным (неинформативным), бесформенным и/или безыдейным.

За счет психосоциального насилия, атакующий пытается подавить волю, сломить сопротивление и покорить атакуемое государство, во всевозможных принадлежностных пространствах. Наверное, в Стратегии национальной безопасности Российской Федерации от 02.07.2021 необходимо ввести раздел о психосоциальной безопасности. Отметим, что в ней используются категории информационно-психологического воздействия и манипулирования.

Сфера виртуально-информационного пространства стала сферой, в которой недружественные субъекты продуцируют напрямую, опосредовано через прокси и/или

косвенно через окружение, а также с помощью смарт-систем негативные инцидентные ситуации, виртуальные сущности которых могут воздействовать как минимум на один элемент целевой ситуации (на субъекта, объект (ресурс) и/или инструмент (средства (элементы телеком-интернет-инфраструктуры и/или связанные с ней элементы инфраструктур), институты и/или допущения). В качестве субъекта может выступить человек, организационная структура и/или орган публичной власти. Целью психосоциальной атаки с помощью знак-продуктов (медиа-продуктов) в виртуально-информационном пространстве является психосоциальная позиция как минимум одного человека, которую необходимо дез-позиционировать (рас-синхронизировать, дезориентировать и/или изменить идентичность), а также дезорганизовать и/или дезадаптировать. Осуществить это можно с помощью явного психосоциального воздействия на сознание и/или память как минимум одного человека и/или неявно минуя их, на всю психику, включая неосознаваемую составляющую, с целью доведения внутреннего состояния людей до критических значений, когда они добровольно и массово начнут переходить в иную принадлежность, не осознавая, что ими манипулируют. Это достигается за счет определенного преимущества в телеком-интернет-инфраструктуре и смарт-системах, позволяющих транснациональным медиа-корпорациям доминировать в виртуально-информационном пространстве за счет продуцирования, распространения негативного контента и/или фильтрации нежелательного для них контента.

БИБЛИОГРАФИЯ

1. *Ильницкий А. М.* Стратегия ментальной безопасности России // Военная мысль. — 2022. — № 4. — С. 24–35.
2. *Макаров Е.* Ментальная и когнитивная войны — вопросы определения, цели и средства // Геополитика.ru. — URL: https://www.geopolitika.ru/article/mentalnaya-i-kognitivnaya-voyny-voprosy-opredeleniya-celi-i-sredstva?ysclid=m5k1d6czeq891503478 (дата обращения: 20.03.2025).
3. *Румянцева В. Г.* Государственный интерес: власть суверена по умолчанию // Вестник МГЮА. — 2023. — № 11. — С. 165–170.
4. Air-Force General Eric Autellet, Dr. Norbou Buchler et al. Cognitive Warfare Symposium. ENSC // NATO Science and Technology Organization. — 2021. — URL: https://2050.su/cognitive-warfare-the-future-of-cognitive-dominance/?ysclid=m5kovrrhds752346147 (дата обращения: 20.03.2025).
5. *Cao K., Glaister S.* et al. Countering cognitive warfare: awareness and resilience // NATO Review. (20 May 2021). Johns Hopkins University & Imperial College London. — URL: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html (дата обращения: 20.03.2025).
6. *Claverie B., Cluzel F.* The Cognitive Warfare Concept // NATO Allied Command Transformation / Innovation Hub. — 2021. — URL: https://2050.su/the-cognitive-warfare-concept/?ysclid=m5kopvahv450540445 (дата обращения: 20.03.2025).
7. Norton B. Behind NATO's «cognitive warfare»: «Battle for your brain» waged by Western militaries // Grayzone. — 2021. — № 8. — URL: https://thegrayzone.com/2021/10/08/nato-cognitive-warfare-brain/ (дата обращения: 20.03.2025).

REFERENCES

1. Ilnitskiy AM. The Strategy of Mental Security of Russia. *Voennaya mysl*. 2022;4:24-35. (In Russ.).
2. Makarov E. Mental and Cognitive Wars — Questions of Definition, Goals, and Means. *Geopolitika.ru*. Available at: https://www.geopolitika.ru/article/mentalnaya-i-kognitivnaya-voyny-voprosy-opredeleniya-celi-i-sredstva?ysclid=m5k1d6czeq891503478 [Accessed 20.03.2025].

3. Rumyantseva VG. The State Interest: the Sovereign's Power by Default. *Courier of Kutafin Moscow State Law University (MSAL)*. 2023;1(11):165-170. (In Russ.).
4. Air-Force General Eric Autellet, Dr. Norbou Buchler, et al. Cognitive Warfare Symposium. ENSC. *NATO Science and Technology Organization*. 2021. Available at: https://2050.su/cognitive-warfare-the-future-of-cognitive-dominance/?ysclid=m5kovrrhds752346147 [Accessed 20.03.2025].
5. Cao K, Glaister S, et al. NATO Review. (20 May 2021). Johns Hopkins University & Imperial College London. Available at: https://www.nato.int/docu/review/ articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html [Accessed 20.03.2025].
6. Claverie B, Cluzel F. The Cognitive Warfare Concept. NATO Allied Command Transformation. *Innovation Hub*. 2021. Available at: https://2050.su/the-cognitive-warfare-concept/?ysclid=m5kopvahv450540445 [Accessed 20.03.2025].
7. Norton B. Behind. NATO's 'cognitive warfare': 'Battle for your brain' waged by Western militaries. Grayzone. 2021;8. Available at: https://thegrayzone.com/2021/10/08/nato-cognitive-warfare-brain/ [Accessed at: 20.03.2025].