Окончание статьи, а также законодательные акты и стратегические документы, использованные в работе, будут опубликованы в № 2/2021.

Литература

1. Арабаджийски Н. Государственное и публичное управление. София: Новый болгарский университет, 2014.

2. Арабаджийски Н. Политика устойчивого развития администрации исполнительной власти в Республике Болгария в Первый программный период членства в Европейском союзе. Сборник докладов научной конференции «Региональная экономика и устойчивое развитие». Т. 2. Варна: Изд. «Наука и экономика» Экономического университета, 2018.

3. Арабаджийски Н. Политика развития администрации исполнительной власти в Республике Болгария в течение Второго программного периода членства в Европейском союзе. Сборник «10 лет Болгарии в Европейском союзе – влияние на развитие публичной политики и законодательства». София: Новый болгарский университет, 2018.

4. Георгиев Л. Региональная экономика. София: Новый болгарский университет, 2009.

5. Георгиев Л. Региональные и муниципальные несоответствия. София: Новый болгарский университет, 2012.

6. Гылыбинова Юл. Европейские регионы – формальное исследование номенклатуры или использование возможностей сближения. София: Новый болгарский университет, 2015.

О проблеме обеспечения когнитивной безопасности

On the Problem of Ensuring Cognitive Security

(DOI: 10.34773/EU.2021.1.24)

Н. МИРОНОВА

Миронова Наталия Геннадьевна, канд. филос. наук, доцент кафедры управления информационной безопасности Института истории и государственного управления Башкирского государственного университета. E-mail: om_aks@mail.ru

Россия вовлечена в информационные связи глобальной коммуникационной среды, являясь объектом пристального внимания спецслужб других стран, объектом и участником информационного противодействия, экономической конкуренции. Риски, обусловленные указанными угрозами, можно отнести к когнитивным. В статье анализируются когнитивная сфера общества как предмет информационной, в частности, когнитивной безопасности, методы когнитивной войны и когнитивные угрозы; обозначен круг проблемы когнитивной безопасности, предложены направления реализации мер когнитивной безопасности.

***Ключевые слова**: когнитивная война, информационная война, когнитивная безопасность.*

Russia is involved in the information links of the global communication environment, being the object of close attention of the special services of countries, the object and participant of information countermeasures, economic competition. The risks associated with these threats can be classified as cognitive. The article analyzes the cognitive sphere of society as a subject of information, in particular, cognitive security, methods of cognitive warfare and cognitive threats; the circle of the problem of cognitive safety is outlined, directions of implementation of measures of cognitive safety are proposed.

***Key words**: cognitive warfare, information warfare, cognitive security.*

Современная политическая реальность насыщена военным противостоянием в разнообразных формах, одна из которых – информационная война, имеющая ныне повсеместный, всепроникающий и постоянный характер благодаря глобальным коммуникациям. Цифровые СМИ

и сетевые технологии стали инструментом эффективного когнитивного и политического воздействия на умы и поведение населения всех стран. Одновременно с развитием информационно-коммуникационных технологий по заказу военных ведомств и корпораций, силами западных thinktank'ов активно ведутся проектные разработки в области социальных, когнитивных технологий, которые находят военное применение. Страны-участники этой «гонки вооружений» (в их числе Россия) отмечают растущие проблемы информационной и когнитивной безопасности. Можно говорить о перерастании информационных войн (information warfare – IW) в новую фазу когнитивной войны; особенность этой фазы IW – масштабы и глубина проникновения в социальную практику и жизнь человека интернета поколения WEB 3.0 (интернет вещей, индустрия 4.0) и когнитивных технологий, дающие тем, кто владеет этими технологиями и каналами на правах создателей, огромное и разнообразное влияние на мировые процессы.

Термин «информационная война» впервые определен в 1990-е в военных стратегических документах; так, в директиве DODD 3600 Минобороны США, «Объединенной доктрине информационной войны», термин «информационная война» (ИВ) определяется как система действий для достижения информационного превосходства в поддержке национальной военной стратегии посредством воздействия на информацию и информационные системы противника. Среди инструментов ИВ – психологические операции для оказания воздействия на системы управления и принятия решений противника, дезинформации, дезорганизации и разрушения его социальных институтов и др. Психологические операции (операции влияния (IO, influence operations), психологические операции (psyop)) обычно понимаются как система мероприятий по распространению подготовленной информации для воздействия в нужном ключе на эмоциональное состояние, мотивацию, принимаемые решения, поведение политических противников и союзников. Психологические операции могут быть также направлены на повышение привлекательности в глазах населения или элит страны-противника; «мягкая сила» как средство воздействия привлечением, убеждением и «подталкиванием» социальных групп страны-противника – широко применяемый способ «добиваться желаемого на основе добровольного участия союзников, а не с помощью принуждения или подачек» (как его определил в 1990 г. автор термина Джозеф Най); на практике конечной целью применения стратегий «мягкой силы» становятся дестабилизация экономической, социальной, духовной жизни (по словам дипломата А.В. Демидова [2, *88*]), через вмешательство во внутренние дела, управление общественным мнением и сознанием целевых групп населения страны-объекта.

То обстоятельство, что подобные «информационные операции» нацелены на сознание, убеждения, процессы мышления и другие когнитивные свойства индивидов, позволяют выделить в особую группу когнитивные операции, и ввести термин «когнитивная война» для обозначения объединенной общим замыслом совокупности когнитивных операций, обособленной во времени от других форм ИВ (таких, как прямое физическое разрушение информационной технической инфраструктуры противника и иное киберфизическое воздействие на информационные каналы). И когнитивные войны нельзя считать чем-то совершенно новым. Как технологии и практика воздействия на морально-волевое и идейное состояние армии, элиты и населения противника, они известны давно, с тех пор как СМИ (печать, радиосвязь, телефон и кинематограф), получив распространение, были превращены государствами в инструмент политической и военной борьбы, проведения «информационных операций» в мирное и военное время как во внешнем контуре, так и для внутреннего употребления.

Когда объектом разрушительного воздействия выступает индивидуальное и коллективное сознание, а конечные задачи воздействия носят политический характер, следует говорить о когнитивной войне. Объектами воздействия в когнитивных войнах становятся культурное и ментальное «пространство» противника: индивидуальное, групповое и коллективное сознание, системы образования и воспитания, коммуникативная практика, социальные ценности, мировоззренческие, научные, конфессиональные представления, поддерживающие целостность социальных структур.

Термин «когнитивная война» употребляется на Западе в более узком смысле, чем «информационная война». Например, «когнитивная война – это изменение с помощью информационных средств того, как думает целевая группа населения и как она действует» [9]; как «манипулирование публичным дискурсом со стороны внешних элементов, стремящихся подорвать социальное единство или политическое доверие к политической системе» [15]; как «процесс дезинформации, направленный на психологическое истощение получателей информации» [14]. В отечественной литературе термин употребляется в социальном контексте редко и в более вольной трактовке, например, В. Лепехин использует термин «когнитивная война» как «война знаний и смыслов» [5]. (Г. Почепцов, например, использует словосочетание «социетальная война» в контексте «война смыслов»).

Субъекты когнитивной войны – государства и их союзы, негосударственные структуры, корпоративные и финансово-политические группы (банковские группы, преступные сообщества, экстремистские организации), иные заинтересованные группы, использующие когнитивные технологии и информационные операции как средство реализации своих интересов и целей.

Объекты воздействия когнитивных войн и операций – социальные структуры, индивидуальное и коллективное сознание (в первую очередь ценностно-смысловое ядро менталитета). Повреждению подвергаются ценностно-понятийная система, мировоззренческие установки, язык как средство коммуникации, традиции, образ и направленность мышления индивидов и целых групп, интерпретации ими событий, логика рассуждений. Указанное «повреждение» отражается на формах и содержании социальной деятельности – системах управления и принятия решений, социальных связях, практиках. С распространением интернета и мобильных гаджетов когнитивное «давление» на убеждения и поведение людей усилилось, а количество каналов информационного воздействия возросло, оказывая запланированное стратегами ИВ воздействие на содержание внимания, мышления, памяти, на эмоции и психические процессы, на ценностно-мотивационный комплекс личности, наконец, а через социальную коммуникацию – и на коллективное сознание и поведение. «Средний» россиянин постоянно погружен в эмоционально и информационно насыщенную среду, достаточно агрессивно воздействующую на сознание и подсознание.

Инструментами когнитивных войн выступают, во-первых, средства информационного воздействия (инструменты и методы политической и религиозной пропаганды, иные информационные операции; «продукция» шоу-бизнеса и кинематографа, СМИ, литература (научная, популярная, художественная), интернет-сервисы (соцсети, браузеры поисковой выдачи, новостные ресурсы и т.д.), развлекательно-спортивные массовые мероприятия и т.д.). Во-вторых, инструментом когнитивных войн и операций выступает институциональная деятельность (деловая и трудовая практика и коммуникация, политическое лоббирование разрушительных по своим социальным последствиям законопроектов, финансирование деструктивной деятельности и социальной активности, непродуманная, противоречивая или деструктивная реформаторская деятельность органов управления и корпоративных структур).

В арсенал технологий, применяемых в когнитивной войне, входят и т.н. «подрывные технологии». Термин «подрывные инновации/технологии» (disruptive innovation [4]) обычно используется в экономическом контексте: как технологические новшества, которые позволяют их обладателю завоевать рынок продуктов или услуг, быстро вытеснив конкурентов за счет привлечения их клиентов качественно новыми потребительскими свойствами товара или услуги. По мере приватизации и «капитализации» культуры, социальных институтов (образования, науки, государства т.д.) последние играют преходящую социальную роль поставщиков коммерческих услуг потребителю, конкурируя на региональном и глобальном рынке друг с другом, с корпорациями за получение прибыли и власть над «рыночным сегментом». В процессе рыночной конкуренции социальные институты в своем новом качестве вынуждены вести технологическую борьбу, и терпят в ней потери от подрывных технологий конкурентов, в первую очередь корпораций с более широким бизнес-опытом и изначально иными, чисто «экономическими» ценностями. Автоматизация и цифровизация, информационно-коммуникационные технологии

(ИКТ) оказались для традиционных социальных институтов и практик «подрывными технологиями», разрушая их. Исчезают бумажные СМИ (как и весь документооборот, они стали электронными) и традиционная издательская деятельность, кинематограф все больше уступает сетевому массовому видео-контенту; институты образования перестают играть ту роль, в которой они стали привычны за последнее столетие (как средство воспитания, передачи технологий, знаний, ценностей национальной культуры от старшего поколения – молодому). Образование стало бизнесом по продаже образовательных услуг с элементами развлекательности (игрификация, тьюторинг и интерактивные учебники вместо учителя, облегченный формат платформенного, ни к чему не обязывающего дистанционного образования); образовательные учреждения вступают в конкуренцию с бизнес-компаниями (которые теперь также предлагают обучение как услугу); государственное управление приобретает черты корпоративно-проектной и сетевой культуры и т.д. Даже институт семьи также испытывает на себе разрушительное воздействие «подрывных цифровых технологии», поскольку большая часть межличностной коммуникации теперь опосредуется гаджетами, телекоммуникационными сервисами, мессенджерами, а родители в таких условиях перестают быть для собственных детей авторитетом и источником опыта, традиционных ценностей, стандартов, образцов поведения. Дети усваивают вестернизованный контент из Интернета, созданного по заказу военных США как раз для информационных задач боевых операций. Л. Харрисон и С. Хантингтон отмечали [13], что вестернизация культурной практики способствует эрозии бытовых и поведенческих норм, культурных и моральных ценностей, косвенно способствуя размыванию национального суверенитета стран. Так цифровые технологии трансформируют «социальную ткань» на всех уровнях, способствуя отчуждению поколений, пресекая преемственность культурного опыта между поколениями народа.

Наиболее широко практика информационных операций до 2000-х гг. применялась государствами при решении внутри- и внешнеполитических задач. Субъект когнитивной войны, решающий свои политические и экономические задачи, стремится к нейтрализации и подчинению политического противника – через навязывание последнему своих стандартов, идеологий, идентичностей, приоритетов развития, ценностей, моделей поведения. Для их укоренения атакуется и хаотизируется духовно-нравственная и ценностная сфера, внедряются чуждые или деструктивные модели поведения, неадекватные культурным и экономическим условиям цели и убеждения (например, бездетность, потребительство и т.п.). Признаками поражения общества в когнитивной и информационной войне могут служить массовая эмиграция (в т.ч. «утечка умов», непродуктивная канализация пассионарности), спад численности населения страны-противника (из-за утраты смыслов, экономических проблем, злокачественного образа жизни, связанного с упадком социальных институтов (семьи, здравоохранения и т.д.), деградацией экономической инфраструктуры, научно-технологическим регрессом). Другие признаки – утрата социальной идентичности, хаотизация и распад социальных связей, как одно из следствий – эсхатологические и упаднические настроения, неспособность к коллективному усилию. Некоторые исследователи [7] также указывают среди видимых признаков проигрыша в информационной (когнитивной) войне «включение информационной системы проигравшей стороны в решение задач в интересах победителя, который определяет входные данные; информационная система проигравшей стороны поглощается структурой победителя и начинает работать в его интересах».

Инструменты когнитивного влияния широко используются и внегосударственными структурами (криминалом, ТНК, надгосударственными структурами, такими, например, как Всемирная организация здравоохранения (ВОЗ) или Всемирный экономический форум (ВЭФ), стремящимися влиять на политику и социальные институты в соответствии с собственными интересами). Так, в течение последнего десятилетия реализуется проект ВЭФ «Глобальная инициатива преобразования» (Global Redesign Initiative, 2009, затем 2016) (варианты прочтения: «глобальная реорганизация», «глобальная перезагрузка») [12]. Этот глобалистский проект «корпоративного толчка к новой форме глобального управления» и изменения ролей государств, корпораций и международных организаций гражданского общества в глобальном

управлении, ставит в центр будущей системы управления ТНК, а не государства, как прежде. Планы подобного масштаба предполагают с их стороны широкомасштабные действия по подведению мировой экономики (и общественного бытия и сознания) к состоянию, после которого и станет возможна «перезагрузка» и перехват управления. Эти действия, по-видимому, дают установиться новой, «сломанной», нормальности, которую можно наблюдать в последние годы и месяцы: сворачивание привычных гражданских свобод, прав и гарантий, усиление цифрового контроля, утрата приватности частной жизни, рукотворная стагнация («локдауны» 2020 года) экономического и социального развития, активное реформирование социальных институтов в направлении, которого, кажется, никто не понимает и мало кто принимает.

В условиях информационного противодействия (в т.ч. когнитивной войны за лояльность населения к политическим элитам) национальное государство для самосохранения и выживания должно, полагаем, следовать собственной стратегии, с учетом явных и предполагаемых угроз, – информационных и когнитивных, учитывая тенденции развития науки и технологий. Когнитивные угрозы – виды, механизмы и источники возможного ущерба основе социального бытия нации, страны, государства. Культурная матрица – ценностное ядро этого бытия, родовое, народное представления о правде, справедливом, разумном, этичном (в высоком и консервативном, а не сиюминутном понимании этих концептов). Культурная матрица поддерживает жизнеспособность народа в истории. Сохранность культурной матрицы от когнитивных атак – сфера когнитивной безопасности государства. У каждой страны система непреходящих, «витальных» ценностей апробируется собственным историческим опытом. (Так, аналитический центр Heritage Foundation в США констатировал, что процветание этой страны зиждется на системе ценностей, среди которых главные – свобода, ответственность, семья, наследие, истина, вера, патриотизм, верховенство закона, самоуправление, предпринимательство, конкуренция).

Когнитивные угрозы как одна из сторон социально-политической практики, реализуемой через технологические инструменты, стали актуальной задачей обеспечения национальной безопасности, в т.ч. информационной безопасности. Понятию «информационная безопасность» в доктрине информационной безопасности РФ придается следующий смысл: «информационная безопасность Российской Федерации – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [3].

Когнитивная безопасность не совпадает с понятием «информационная безопасность», не укладывается полностью в содержание последнего и имеет более конкретное содержание. Когнитивную безопасность мы понимаем как состояние сохранности и защищенности фундаментальных (для индивидуального и социального сознания) ценностей, когнитивных и поведенческих моделей, которые имеют «сберегающее» содержание по отношению к социальной практике, позволяя обеспечить жизнеспособность, «витальность» как индивида, так и социума, способность последнего эффективно решать коллективные задачи, противостоять внутренним и внешним вызовам и конфликтам. Понятие и методология когнитивной безопасности (как совокупности средств и мер противодействия угрозам) требуют глубокого анализа. О.Н. Новокшанов определяет когнитивную безопасность как «состояние когнитивной сферы, обеспечивающей эффективность и результативность деятельности человека, направленной на удовлетворение его потребностей и реализацию интересов» [6, *136*]. Понятием, близким термину «когнитивная безопасность», является термин «социетальная безопасность» (societal security), определенный его авторами довольно широко, – как «способность общества сохранять свою сущность в изменяющихся условиях и при возможных или явных угрозах» [10]. В стандартах безопасности [1] социетальная безопасность трактуется как защита общества от инцидентов, чрезвычайных ситуаций и бедствий, вызванных умышленными и неумышленными действиями человека, опасными природными явлениями и техническими неисправностями,

а также реагирование на такие события. Г. Почепцов использует термин «когнитивная безопасность» как нечто, что «должно защитить нас от навязываемого извне понимания ситуации, чужого и чуждого стиля мышления».

Методология и задачи когнитивной безопасности должны отвечать на вызовы так называемых когнитивных войн, объектом которых является социум на различных уровнях организации и социальное сознание. Средства ведения когнитивной войны имеют широкий арсенал уже ставших традиционными технологий. К ним относятся воздействие на сознание (словесное, визуальное, с использованием иных сигнальных систем) методами внушения и НЛП, пропаганды и контрпропаганды, отвлечения, манипулирования; конструирование мифов, ложных убеждений, симулякров, «медиавирусов»; технологии постепенного изменения коллективных убеждений и практик («окна Овертона»), методы, задействующие психологические и биосоциальные «механизмы» (конформность, психическое заражение, искажение восприятия и внимания); внедрение антисоциальных, контрпродуктивных и деструктивных моделей поведения, разрушение языка как основы мышления и коммуникации (внедрением иноязычной терминологии, популяризацией обсценной лексики, нарочитым искажением структуры речи и безграмотностью). Можно упомянуть технологии меметической инженерии (проекта Social Mediain Strategic Communication от DARPA и других многочисленных подобных проектов, выполненных по заказу военного ведомства США для обеспечения информационных войн). Подобные когнитивные операции А. Грамши назвал «молекулярной» агрессией в культурное ядро. Кроме социальных технологий, управление когнитивной сферой исследуется в физике, нейронауках, медицине и химии, кибернетике; в когнитивных войнах знания и технологии этих наук также используются для создания требуемого психического, эмоционального состояния: транквилизаторы, наркотические, медикаментозные средства массово применялись с целью снизить уровень социальной напряженность и агрессии в обществе – или, наоборот, спровоцировать группы на разного рода политическую активность (со стороны США эти средства применялись в отношении населения враждебных стран в ходе «цветных» революций). В будущем арсенал инструментов воздействия на ментальную сферу обещает пополниться кибертехнологиями прямого воздействия на работу мозга; так, значительные усилия направлены на разработку нейроинтерфейсов [8; 11], технологий реалистичной виртуальной реальности, неотличимой для пользователя от действительности, прямого радиочастотного воздействия через мозговые структуры на сознание и поведение человека и т.д.

Возможные меры противодействия когнитивным угрозам:

– усилия по информационной безопасности (в т.ч. кибербезопасности);

– совершенствование методов распознания дезинформации и противодействия ей; данная задача значительно усложняется в настоящее время, когда к созданию фейкового контента (включая новостные, научные публикации, видео-контент) привлекаются нейросетевые технологии (пример: подделка мультимедийного контента deepfake);

– ограничение доступности некоторых каналов, через которые осуществляется воздействие деструктивного и манипулятивного контента;

– создание собственных каналов когнитивного и информационного воздействия для решения оборонных задач;

– развитие методов и технологий прогнозирования рисков в области информационной и когнитивной безопасности;

– проактивная стратегия и тактика России во внешнеполитической деятельности с использованием своих когнитивных технологий и стратегий «мягкой силы»;

– выработка объединяющих и убедительных национальных смыслов, приоритетов и задач, способных придать импульс национальному развитию, мотивирующих широкие круги российского общества, в первую очередь, для молодого поколения;

– практическое обеспечение условий для реализации социальной справедливости как одной из основ социальной устойчивости российского общества.

Литература

1. ГОСТ Р 22.0.12-2015/ИСО 22300:2012 Безопасность в чрезвычайных ситуациях. Международные термины и определения.

2. Демидов А.В. От «мягкой силы» к «управляемому хаосу» // Геополитический журнал. 2014. № 4. С. 86–93 [Электронный ресурс]. URL: https://www.elibrary.ru/download/elibrary_23199886_95216500.pdf

3. Доктрина информационной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. [Электронный ресурс]. URL: http://kremlin.ru/acts/bank/41460

4. Кристенсен, К. Дилемма инноватора: как из-за новых технологий погибают сильные компании. М.: Альпина Паблишер, 2015. 239 с.

5. Лепехин В. Что такое когнитивная война и можно ли в ней победить // РИА Новости, 2020. [Электронный ресурс]. URL: ria.ru/20160426/1420518962.html

6. Новокшанов О.Н. Когнитивная безопасность и информационно-аналитическое противодействие // Право и государство: теория и практика. 2015. № 9. С. 132–137 [Электронный ресурс]. URL: https://www.elibrary.ru/download/elibrary_24277628_37940652.pdf

7. Попова С.В., Федоринов В.Е. Цели и последствия информационной войны // Воздушно-космические силы. Теория и практика. 2018. № 6. С. 15–21.

8. Слияние человека и машины. Neuralink [Электронный ресурс]. URL: https://habr.com/ru/post/517058/

9. Backes, O., Swab, A. Cognitive Warfare (The Russian Threat to Election Integrity in the Baltic States. Harvard Kennedy School, 2019. 66 p. [Электронный ресурс]. URL: https://www.belfercenter.org/sites/default/files/2019-11/CognitiveWarfare.pdf

10. Buzan B., Kelstrup M., Lemaitre P., Tromer E., Waever O. Identity, Migration and the New Security Agenda in Europe (англ.) рус. Pinter, 1993. 221 p.

11. DARPA заказало разработку мозговых имплантатов высокого разрешения для интерфейса «мозг-компьютер» [Электронный ресурс]. URL: https://www.nanonewsnet.ru/news/2017/darpa-zakazalo-razrabotku-mozgovykh-implantatov-vysokogo-razresheniya-dlya-interfeisa-mozg

12. Gleckman, Harris. Multi-stakeholderism: a corporate push for a new form of global governance; Глекман, Х. Многосторонность: корпоративный толчок к новой форме глобального управления // Отчет о программе Транснационального института (TNI) (19 января 2016) [Электронный ресурс]. URL: https://www.tni.org/en/publication/multi-stakeholderism-a-corporate-push-for-a-new-form-of-global-governance

13. Harrison L., Huntington S. Culture Matters: How Values Shape Human Progress (Харрисон Л., Хангтинтон С. Значение культуры: как культурные ценности формируют человеческий прогресс). N.Y.: BasicBooks, 2000.

14. Mackiewicz D., Cognitive warfare: Hamas & Hezbollah and their insidious efforts // Conference: INSS-Summer Institute 2018At: Tel Aviv, Israel. [Электронный ресурс]. URL: https://www.researchgate.net/publication/ 337228818_Cognitive_Warfare_-_Mackiewicz-Diana_2018

15. Rosner, Y., & Siman-Tov, D. (2018, March 8). Russian Intervention in the US Presidential Elections: The New Threat of Cognitive Subversion. Retrieved September 13, 2018 [Электронный ресурс]. URL: http://www.inss.org.il/publication/russian-intervention-in-the-us-presidential-electionsthe-new-threat-of-cognitive-subversion/