Российский опыт

DOI: 10.23932/2542-0240-2020-13-2-3

«Гибридные угрозы» безопасности России: выявление и противодействие

Светлана Игоревна КОДАНЕВА
кандидат юридических наук, старший научный сотрудник
Институт научной информации по общественным наукам РАН (ИНИОН РАН),
117218, ул. Кржижановского, д. 15, к. 2, Москва, Российская Федерация
E-mail: kodanevas@gmail.com
ORCID: 0000-0002-8232-9533

ЦИТИРОВАНИЕ: Коданева С.И. (2020) «Гибридные угрозы» безопасности России: выявление и противодействие // Контуры глобальных трансформаций: политика, экономика, право. Т. 13. № 2. С. 44–71. DOI: 10.23932/2542-0240-2020-13-2-3

Статья поступила в редакцию 25.01.2020.

АННОТАЦИЯ. *В научной литературе принято рассматривать и анализировать войну исключительно как насильственное (конвенционное) противостояние субъектов международной политики. Однако при этом не учитывается, что современные войны все чаще разворачиваются в «серой зоне», т. е. вне рамок международного права, ведутся они как в физическом, так и в иных измерениях – информационном, кибернетическом, культурном, когнитивном, – в основном невоенными способами и с привлечением иррегулярных формирований (повстанцев, террористов и т. п.). В результате сегодняшнее межгосударственное противостояние становится все более сложным и комплексным – гибридным, представляя новые механизмы неядерного сдерживания.*

Важно понимать, что неумение вовремя распознать ведущуюся противником войну, определить направление удара губило многие государства, начиная с Римской империи и заканчивая СССР. Это определяет актуальность и своевременность настоящего исследования, направленного на анализ содержания феномена гибридной войны, выбор основных применяемых сегодня способов ее ведения и предложение мер противодействия.

Следует признать, что в современной научной литературе нет единого подхода к пониманию того, что собой представляет гибридная война, что вполне объяснимо именно ее сутью – изменчивостью, сложностью и комплексностью способов ее ведения, а также гибкостью и адаптивностью к конкретным обстоятельствам. Существует достаточно много разрозненных исследований, посвященных отдельным составляющим гибридной войны, таким как «мягкая сила», информационная, экономическая и кибервойны, «цветные революции» и т. д., в которых различные авторы используют противоречивые подходы.

Предметом настоящего исследования является феномен гибридных войн, его содержание и конкретные способы ведения таких войн. Целью работы является проведение комплексного ана-

лиза предмета исследования, а также структурирование явлений, образующих в своем комплексе феномен гибридной войны, определение их соотношения и взаимного влияния различных способов ведения гибридной войны, формулирование конкретных предложений по противодействию угрозам национальной безопасности России.

В статье подчеркивается важность выработки комплексных стратегических подходов, направленных, прежде всего, на выявление уязвимостей, а также включающих духовную безопасность как основу всей системы безопасности и противодействия гибридным угрозам.

С учетом указанных предмета и цели во введении раскрывается актуальность исследования феномена гибридной войны и опасность, которую данный вид межгосударственного противостояния представляет для России. Затем анализируются понятие гибридной войны и ее содержание, а также четыре основных способа ее ведения. По результатам проведенного анализа следуют выводы и предложения по противодействию угрозам национальной безопасности России.

КЛЮЧЕВЫЕ СЛОВА: *гибридные войны, гибридные угрозы, мягкая сила, информационная война, информационная безопасность, кибербезопасность, социальные сети, критическая инфраструктура, национальная безопасность*

Введение

Сегодня мир стремительно меняется под воздействием современных технологий, которые во многом сближают людей всего земного шара. Действительно, с помощью сети Интернет мы можем общаться с любым человеком в любой точке света, обмениваясь мгновенными сообщениями. С одной стороны, это делает нашу жизнь более свободной и удобной. С другой стороны, размываются национальные границы и, что значительно важнее, традиции государств. Глобализация очень широко обсуждается в современной научной литературе в самых разных аспектах. Однако в настоящей статьей мы предлагаем обратиться к исследованию последствий глобализации и массового распространения современных технологий для безопасности государств.

Прежде всего речь идет о формировании единого мирового информационного пространства, которое кардинально меняет духовную жизнь общества и выступает одним из ключевых факторов формирования нового национального самосознания. Современные СМИ и социальные сети позволяют создавать и передавать на любые расстояния информационные продукты. Россия как часть мировой информационной сети является также активным потребителем подобного контента, формируемого как на территории нашей страны, так и за рубежом. В результате происходит интенсивный процесс межкультурных коммуникаций, и следует признать, что Россия не столько предлагает миру свои культурные ценности, сколько потребляет предложенные Западом ценностные образцы, которые уже довольно прочно укоренились в российском национальном сознании.

Давно известно, что подобное воздействие является частью «мягкой силы» – метода влияния на иностранные государства с целью навязывания им своих ценностей и идеологии. Безусловно, главным источником такой «мягкой силы» являются Соединенные Штаты Америки, успешно распространившие по всему миру свои «либеральные ценности». Однако, к слову сказать, Китай стремится к тому, чтобы на

равных конкурировать с США на данной почве, активно инвестируя в распространение своих культурных ценностей по всему миру [Политика «мягкой силы» Китая в Азии 2019].

Как указано в Концепции внешней политики РФ, инструменты «мягкой силы» все активнее используются в международной политике для решения различных внешнеполитических задач. Эти инструменты включают в себя различные способы иностранного влияния на гражданское общество, информационно-коммуникационные и социальные системы государств. На решение военных, политических, экономических конфликтов в международных отношениях все активнее влияют информационные приемы формирования общественного мнения, финансово-экономические технологии внедрения массовых стандартов, продвижение культурно-исторических оценок моделей национального развития, рейтинговые оценки финансовой и социальной стабильности [*Ступаков* 2018]. Эти гибридные методы воздействия крайне разнообразны, гибки и довольно легко адаптируются для различных задач.

Не случайно специалисты все активнее говорят о нарастании так называемой гибридной войны. Это явление все активнее используется в противоборстве между государствами, становится все сложнее и многограннее, что связано с опасностью (для всей цивилизации) применения современных достижений в области военной техники, которая развивается так стремительно, что риск уничтожения всего человечества в случае столкновения крупных и сильных в плане военного оснащения государств все больше возрастает. В результате человечество должно либо вообще отказаться от разрешения возникающих конфликтов военным путем, либо способы противостояния должны трансформироваться. Поэтому современные конфликты становятся все более сложными и комплексными, в них все реже задействуют непосредственно военную силу. Мы имеем дело с современным видом межгосударственного противостояния и эффективным инструментом стратегического неядерного сдерживания, предполагающим беспрецедентное сочетание комплекса мер силового и несилового воздействия на противника в реальном времени.

Современная война переходит из мира реального в мир виртуальный – киберпространство, где разворачивается настоящее противоборство сверхдержав; более того, война из явления сугубо физического все больше переходит в духовную и идеологическую плоскость, когда современные технологии используются для управления массовым сознанием; наконец, глобальный финансовый и особенно банковский сектора предоставляют серьезные экономические рычаги влияния на государство.

Понятие «гибридная война» и основные способы ее ведения

Термин «гибридная война», все более активно используемый в современной политической риторике, появился в 2007 г. в США[1], хотя среди специалистов до сих пор не сформировалось единого определения данного явления. На сегодняшний день можно выделить три основных подхода. В соответствии с первым, гибридная война – это совокупность враждебных действий одного государства в отношении друго-

1 Авторство принадлежит научному сотруднику Министерства обороны США Ф.Г. Хоффману, который сформулировал классическую концепцию гибридной войны.

го, а также разнообразная военная, финансово-экономическая и общественно-политическая поддержка противников правящего режима [*Williamson, Mansoor* 2012][2].

При втором подходе гибридная война подразумевает сочетание вооруженных и невооруженных действий одного государства в отношении другого (данный подход скорее относится к операциям, носящим гибридный характер, когда военные действия сопровождаются, например, информационными атаками. Именно по такому сценарию была проведена операция в Косово). Одним из наиболее признанных определений гибридной войны при данном подходе является формулировка Международного института стратегических исследований Military Balance, согласно которой «гибридная операция – это использование военных и невоенных инструментов в интегрированной кампании, направленной на достижение внезапности, захват инициативы и получение психологических преимуществ, использование дипломатических действий, масштабные и стремительные информационные, электронные и кибероперации, прикрытие и сокрытие военных и разведывательных действий в сочетании с экономическим давлением» [*Кучинская* 2018, с. 123][3].

Наконец, третий подход – комплексный, при котором определение гибридной войны складывается из ключевых особенностей обоих подходов, – это совокупность разнообразных невооруженных враждебных действий с ограниченным использованием, при необходимости, вооруженных сил специального назначения; сочетание мультимодальных и многовариантных действий и конфликтов [*Hoffman* 2009][4]. Так, к способам ведения гибридной войны можно отнести:

– политическое давление на международной арене;
– экономические санкции;
– информационные войны;
– кибервойны;
– деятельность спецслужб на территории противника, спонсирование оппозиции, сепаратистов, а также террористических организаций, действия, направленные на повышение преступности (например, наркоторговли и торговли оружием, людьми, вовлечение несовершеннолетних в преступный бизнес и т. д.)[5].

Таким образом, суть современной гибридной войны заключается в:

– использовании «мягкой силы», основанной на экономическом и политическом влиянии;
– экономическом «закабалении» противника и экономических войнах;
– применении современных технологий пропаганды и информационной обработки населения противника; создании информационных агентств на территории противника и/или расширении вещания подконтрольных СМИ среди местного населения с целью донесения иного взгляда на общественные процессы и форми-

2 Данного подхода также придерживаются Кучинская М.Е. [*Кучинская* 2018], Ford Ch.M., Williams W.S. [*Ford, Williams* 2018] и др.
3 Данного подхода также придерживаются Ладыгин Ф.И., Афанасьев С.В. [*Ладыгин*, *Афанасьев* 2017], Фролов А.В. [*Фролов* 2019] и др.
4 Данного подхода придерживается НАТО [The Secretary General's Annual Report 2018], Hunter E., Pernik P. [*Hunter, Pernik* 2015], MCDC [Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces 2019] и др.
5 Так, А.В. Панова приводит пример, когда с помощью технологий информационной войны в подростковую культуру внедряются элементы культуры криминальной, идеология банды, которая должна жить по воровским законам [*Панова* 2019].

рования искаженного восприятия действительности, дискредитации политического лидера и руководства страны (информационная война);
– кибератаках на объекты критической инфраструктуры, органы власти, финансовые учреждения с целью нарушения их нормального функционирования, разрушения экономической основы существования государства; психологическом давлении на население противника (как часть информационной войны);
– выдвижении агентов влияния из местного населения, оказании им финансовой и организационной поддержки с целью организации протестных акций, провокаций власти и массовых мероприятий, дискредитирующих правительство; по возможности – организации гражданского неповиновения, массовых беспорядков, «цветных революций»;
– создании и поддержке сепаратистских и террористических организаций, разжигании «партизанских» войн, криминализации общества.

При этом гибридная война предусматривает три стадии [*Брычков и др.* 2019]:

1. Расшатывание ситуации.
2. Деградация, разорение и распад страны с ее превращением в «недееспособное» государство.
3. Смена политической власти.

Таким образом, гибридная война предполагает интеграцию различных реальных и виртуальных угроз (дипломатических, военных, экономических, информационных и т. д.) с целью психологического воздействия на государство-жертву, погружение его в ситуацию неопределенности, ослабление и разрушение без объявления войны, а также на создание вокруг него соответствующего информационного поля, призванного сформировать у мировой общественности такой образ данного государства, который оправдывал бы любые недружественные и даже агрессивные действия в его адрес.

Очевидно, что Россия, а ранее Советский Союз были жертвами такой войны, проводимой США. Так, на международной арене постоянно проводятся акции, направленные на уменьшение международного влияния России, ее изоляцию. Причем акции эти могут проводиться в самых разных сферах, например, к таковым можно отнести отстранение российских спортсменов от участия в Олимпиаде, разжигание допинговых скандалов, раскол православия на Украине или постоянное блокирование в Совете Безопасности ООН любых решений, предлагаемых Россией. В экономической сфере – это санкции, а также ограничение доступа российских компаний на зарубежные рынки. В последнее время все более популярным приемом стало переписывание истории, искажение событий Второй мировой войны и роли в ней Советского Союза. Наконец, это прямая пропаганда образа «империи зла» сначала в отношении СССР, а теперь и России. Особенно активно такая пропаганда стала вестись в связи с событиями на Украине, которые привели к присоединению Крыма к России, образованию ДНР и ЛНР.

Характерно, что западные СМИ и политологи возлагают ответственность за разработку и внедрение в практику международных отношений соответствующих технологий, которые характеризуются как вероломные и глубоко аморальные, на Россию (см, например, [*Karlsen* 2019; *Bowman* 2018; *Clas* 2018; *Major, Davis* 2015]).

Инструменты «мягкой силы» как элемент гибридной войны

Основы концепции «мягкой силы» были заложены в 1990-х гг. американским политологом Дж. Наем, который определял ее как способность государства добиваться желаемого результата во внешней политике не столько с помощью принуждения и оказания давления, сколько посредством убеждения и привлечения на свою сторону зарубежной аудитории. Соответственно, первоначально данная концепция состояла из трех элементов: политического курса, ценностей и культуры [*Крячкина* 2019].

Впоследствии она постоянно развивалась и расширялась. Так, если обратиться к рейтингу «мягкой силы» государств The Soft Power 30 2019 г., то в нем нашли отражение не только многочисленные ее источники, но и глобальный политический контекст, включающий как тенденции глобализации и сопровождающего ее ослабления политической власти национальных правительств, при котором негосударственные субъекты играют все бóльшую роль в управлении, так и такие аспекты, как цифровая революция и даже изменение климата. Соответственно, данный индекс учитывает объективные (система управления, уровень цифровизации, культурное наследие, уровень образования, развитие предпринимательства и др.) и субъективные данные (дружелюбность, кухня, люксовые товары, внешняя политика, качество жизни и др.) [The Soft Power 30 2019].

«Мягкая сила» Запада и, прежде всего, Соединенных Штатов Америки традиционно имеет целью «распространить западные ценности и институты, вынуждая другие общества уважать права человека, как их понимают на Западе, и принять демократию по западной модели» [*Брычков и др.* 2019]. Соответственно, основной стратегией США и НАТО является распространение во всем мире универсальных ценностей, включая применение для этих целей силы или угрозы ее применения.

Это неудивительно, поскольку общественное сознание всегда играло ключевую роль в управлении любой страной, являясь воплощением культурной и духовной идентичности нации. И именно поэтому общественное сознание является главной целью для манипулирования. Самый большой прорыв в этом направлении связан с формированием идеологии «общества потребления», которая постепенно стала вытеснять традиционные ценности практически во всех странах мира, заменяя их ценностями массового потребления во всем, начиная от предметов первой необходимости и заканчивая сферой культуры и искусства.

Примечательно, что самым эффективным методом управления общественным сознанием стал маркетинг. Особенно значима его роль в формировании ценностей. Так, еще в 2006 г. М. Симагути писал, что «роль маркетинга заключается в создании из любых социально значимых инновационных ценностей или идей таких комплексных систем, которые легко бы воспринимались обывателями, потребителями, пользователями» [*Симагути* 2006, с. 7]. Именно так маркетинг изо дня в день создает новые ценности, формируя общество потребления, стержнем которого, как известно, является индивидуальное потребление, умело направляемое «рынком» и приводящее к все возрастающей стратификации и неравенству.

Таким образом, манипулирование общественным сознанием происходит с использованием приемов маркетинга. И, к слову сказать, идеология глобализации, активно продвигаемая США, – это один из таких приемов. Глобали-

зация – это процесс всемирной экономической, политической, культурной и религиозной интеграции и унификации. Глобализация подрывает национальную идентичность и самобытность периферийных стран, вытесняет их с глобальных рынков, усиливает технологический и экономический разрыв между бедными и богатыми странами.

Таким образом, глобализация служит важным составляющим еще одной разновидности гибридной войны – войны цивилизационной, логика которой подразумевает, что народ завоеванного государства необходимо раздробить, ослабить и заставить безропотно исполнять волю победителя, причем бóльшую часть этих задач должен выполнить сам этот народ, который посредством искажения его традиционных самосознания, морали и ценностей превращается в толпу, которой легко можно манипулировать при помощи информационных технологий.

При этом доминирование идеологии «общества потребления» как идеологии эгоцентризма, сопровождающееся «вымыванием» традиционных ценностей и социокультурных установок, устраняет сдерживающие механизмы для проявления негативных черт личности, в результате чего в информационном пространстве, особенно в социальных сетях, формируется агрессивная среда, провоцирующая психологическое насилие и социально-психологическую деформацию личности.

Особенно подвержены этому подростки и молодежь, которые чаще пользуются компьютерами и гаджетами для общения и, соответственно, погружены в культуру, где агрессивное поведение считается приемлемым или, по крайней мере, ожидаемым. Киберпространство создает среду, в которой люди чувствуют себя более раскованными в своих эмоциях, словах и поведении, поэтому молодые люди становятся все более зависимыми от виртуальной среды: здесь проще знакомиться, общаться, раскрывая свое истинное «я». Здесь они чувствуют себя вправе говорить и делать то, что обычно не делают в физическом мире, включая издевательства и оскорбления. Новые методы запугивания и преследования в Сети появляются постоянно, часто в новых приложениях или на новых интернет-форумах, что затрудняет борьбу с этим набирающим обороты негативным явлением. По данным последних исследований, почти половина подростков (49%) совершали агрессивные действия в Интернете и более половины (61%) подвергались киберагрессии [*Calpbinici, Arslan* 2019].

Ученые всего мира пытаются найти истоки этой проблемы и способы «лечения», но пока что безуспешно. Сфера безопасности информационного общества пока находится в процессе становления. Но хочется обратить внимание на данные эмпирических исследований, демонстрирующие сдерживающий эффект культуры народа. Так, степень агрессии и ненависти в Сети существенно различаются в разных странах [*Song, Zhu, Liu, Fan, Zhu, Zhang* 2019]. Например, жители восточных стран, чьи культуры характеризуются коллективистскими ценностями, высокой моральной дисциплиной, высоким уровнем эгалитарной приверженности и низким уровнем избегания неопределенности (конфуцианские ценности), демонстрировали более низкий уровень агрессии, чем жители западных стран с менее коллективистскими культурами. Исследование китайских, польских и американских студентов показало, что чем выше индивидуализм в культуре, тем больше склонность к прямому и косвенному агрессивному поведению [*Yuchang, Junyi, Junxiu, Jing, Mingcheng* 2019]. Кроме того, китайские подростки (жертвы и свидетели) чаще

обращаются за помощью к преподавателям, поскольку верят в то, что взрослые могут защитить их.

Не удивительно, что такие страны, как Китай, осознавая опасности, связанные с развитием информационного общества, принимают активные превентивные меры. Так, Председатель КНР Си Цзиньпин все чаще отмечает важность информационной и кибербезопасности: «Отсутствие кибербезопасности – отсутствие национальной безопасности» [*Разумов* 2017].

Следует отметить, что политика «мягкой силы» Китая и вообще азиатских стран несколько отличается от западной, поскольку главной целью для стран Востока является создание, прежде всего, своего позитивного образа в глазах простых людей при сохранении своей культурной и духовной идентичности, поэтому их «мягкая сила» реализуется посредством общественной и культурной дипломатии.

При этом «мягкая сила» Китая направлена не только на граждан других стран, но и на своих соотечественников, проживающих за рубежом, с тем чтобы они разделяли идеологию и фактически стали агентами влияния Китая. Целью политики «мягкой силы» Китая является как пропаганда своей культуры вовне, так и сохранение ее внутри страны, во-первых, в качестве противодействия «мягкой силе» Запада, навязывающего миру свои ценности, а во-вторых, поскольку ценностный вакуум, который не заполняется, приводит к распространению антиценностей, связанных с овеществлением мира, а значит, трансформацией общественного сознания. Для этого, например, Китай инвестирует значительные средства в голливудские кинокомпании, которые снимают фильмы мирового уровня, базирующиеся на традиционных китайских ценностях и культуре, адресованные как жителям других стран (например, мультфильм «Кунг-фу Панда»), так и китайским потребителям. Аналогично сегодня в этой стране активно развиваются средства массовой информации, включая интернет-СМИ, обеспечивающие китайских (и не только) потребителей достаточным объемом высококачественной продукции. В качестве инструментов «мягкой силы» используются и образовательные учреждения, и культурный туризм, и даже центры традиционной китайской медицины.

В целом китайские политологи сформулировали понятие «мягкая сила» как совокупность, в которую входят стратегия развития государства, идентификационная мощь идеологии и доминирующие ценностные ориентации, притягательность социального строя и экономической модели, национальная идея и творческий потенциал нации, обаяние культуры и ее влияние в международных делах [Политика «мягкой силы» Китая в Азии 2019].

В Японии больший акцент делается на успешность экономической модели, причем применительно к экономически развитым странам целью «мягкой силы» Японии является продвижение интересов национального бизнеса, а в отношениях с менее развитыми соседями – демонстрация экономической мощи и гуманитарной зрелости [*Крячкина* 2019].

России сегодня также необходимо серьезно задуматься над разработкой собственной политики «мягкой силы», причем она, как и в случае Китая, должна быть направлена не только на позиционирование страны вовне, хотя это также крайне важно, но и на адекватные меры по защите своей национальной идентичности и духовных основ внутри страны.

Что касается внешней политики, то здесь Россия предпринимает определенные усилия по позиционированию

себя как миролюбивой страны, страны-миротворца, готовой прийти на помощь в случае необходимости (последний пример этого – помощь в борьбе с коронавирусом, которую Россия оказала Италии и США). Однако этого явно недостаточно. Для успешного позиционирования себя в качестве ведущего мирового игрока необходимы три составляющие: экономическая привлекательность, привлекательные идеология и культура, высокий уровень технологического развития. Что касается первой составляющей – это предмет серьезного экономического анализа, по третьему направлению сегодня в России предпринимаются определенные усилия в рамках национальных проектов «Цифровая экономика» и «Наука», об эффективности или неэффективности которых также можно спорить.

Но ключевым элементом, на котором может и должна базироваться серьезная «мягкая сила» страны, является сильная духовная и идеологическая составляющая, которая одновременно будет служить защитой и иммунитетом от воздействия чужой «мягкой силы».

Политика идентичности – важнейший ресурс государства по обеспечению стратегической социально-политической стабильности, информационной безопасности и поддержанию «ценностного суверенитета общества» [*Сургуладзе* 2019].

Однако духовные ценности формируются у человека в самом раннем возрасте. В последние годы очень много говорилось о важности системы образования не просто в обучении, но в воспитании и развитии личности, много писалось о той ошибке, которая была допущена, когда российская система образования отказалась от советской модели, которая закладывала «основы научных знаний и формировала морально-нравственные качества, обеспечивающие доступ к объектам высокого уровня сложности – объектам культуры и науки» [*Сундиев, Фролов* 2019]. Очевидно, что сегодня жизненно важно эту ошибку исправить, вернувшись к прежней системе образования-воспитания. Кроме того, необходимо создание эффективной системы патриотического воспитания молодежи, прививающего ей традиционные российские моральные и духовные ценности, включая любовь к Родине и готовность ее защищать. При этом, безусловно, следует учитывать и реалии сегодняшнего дня, и то, что основную роль в решении этих задач должно играть само общество, поэтому государству следует больше внимания уделять поддержке и развитию социальных инициатив, общественных движений и объединений, цели которых созвучны реализуемым государством направлениям политики идентичности.

Информационная война как элемент гибридной войны

Следует признать, что информационная война – это крайне важная составляющая гибридной войны, направленная на формирование нужного общественного мнения. Ее цель – разложение сил противника и убеждение своих сторонников в том, что противник – преступник, подлежащий уничтожению. Соответственно, информационная война может вестись на двух уровнях: внешнем и внутреннем. Приведенные выше примеры в основном относятся к внешнему уровню – дискредитации страны на международной арене. Также наиболее яркими примерами информационной войны внешнего уровня в последнее время стали скандалы с отравлением экс-полковника ГРУ С. Скрипаля, обвинением России во вмешательстве в выборы Президента США 2016 г., обвинени-

ем российских спортсменов в применении допинга. Все эти скандалы имели своей целью делегитимизацию России на международной политической арене.

Внутренний уровень имеет своей целью психологическое подавление противника, как связанное с нанесением прямого урона с помощью информационного оружия[6], так и со скрытым манипулированием, которое во многом граничит с такими разновидностями гибридной войны, как «мягкая сила» и выдвижение и поддержка агентов влияния, провокация массовых акций гражданского неповиновения, а точнее, служит инструментом для них.

Первый вариант используют, как правило, во время войн или военных операций. Как отмечает Ч. Фриман, «во время войн операции психологического воздействия позволяют добиться быстрого распространения фальшивых электронных сообщений, фейковых новостей, компромата на политических лидеров, в т. ч. посредством социальных сетей. В результате таких действий нарушается политическая координация и процесс принятия решений, искажается общественное представление о ситуации» [*Фриман* 2018].

Соответственно, второй вариант информационной войны направлен на уничтожение духовно-нравственных основ нации, подмену национальных ценностей на «глобальные», т. е., по сути, чуждые, инородные, подавление навыков критического анализа информации, формирование «сетевого общества», легко поддающегося манипулированию. Влияние информационного пространства на общественное сознание сегодня трудно переоценить, и ничего подобного не существовало ранее. Прежде всего, конечно, речь идет об Интернете – универсальном инструменте для общения, а также трансформации и трансляции любой информации на любом расстоянии, но главное – ее доставки конкретному конечному адресату. Речь и о порожденных Интернетом социальных сетях, которые формируют общность людей, сегментированных не по национально-территориальному принципу, а по интересам и приверженности определенным идеям, т. е. вне государственной и институциональной идентичности.

Как показывают исследования, именно в социальных сетях наиболее силен эффект эхо-камеры, при котором нужные идеи и убеждения закрепляются в сознании людей посредством многократного их повторения внутри закрытой системы (клуб единомышленников, блог, сообщество в социальных сетях, субкультура и т. п). Соответственно, участники таких сообществ становятся практически невосприимчивы к внешней информации и иным мнениям, ориентируясь только на членов своей группы. Более того, магистральная логика обсуждений в блоге или группе в социальной сети полностью нивелирует собственные взгляды и убеждения участника обсуждения, тем самым заключая его в изолированной эхо-камере [*Виловатых* 2018].

И если раньше противникам действующего режима (например, диссидентам) было практически невозможно собраться в некое единое сообщество, понять, сколько единомышленников у тебя есть в реальности, и привлекать новых, да и распространение информации в этом сообществе требовало определенных усилий и затрат, связанных с организацией вещания на территории

6 Данный вариант информационной войны был реализован США во время проведения операции в Косово, Афганистане, Ливии, Сирии, войны в Ираке.

чужого государства, печатью «самиздата» и т. д., то теперь достаточно зарегистрироваться в социальной сети, найти определенную социальную группу и вступить в нее. При этом, как было отмечено, социальные сети формируют принципиально новый тип общественного сознания, культивирующий определенную форму общественного взаимодействия; они позволяют не только распространять нужную информацию, формируя определенные события, но и практически мгновенно создавать неких «лидеров мнений», как правило, не имеющих политического бэкграунда. Кроме того, в последнее время получил широкое распространение платный троллинг – размещение в социальных сетях провокационной информации, призванной нагнетать негативную эмоциональную обстановку, а также формировать нужное общественное мнение[7].

Также широко используются в информационных войнах такие приемы, как астротурфинг[8] и мемы[9]. Все они направлены на создание «информационных вирусов» и массовое поражение ими сознания пользователей социальных сетей [*Breden* 2013].

В связи с этим важно понимать, что реагирования на уже происшедшие события или размещенную в Сети информацию сегодня недостаточно, крайне важно обеспечить превентивное создание органами власти информационного поля, отвечающего национальным интересам государства, поскольку это минимизирует негативный эффект, который силы противника достигают, заполняя информационные пустоты и вакуум. При этом следует учитывать, что доверие людей к традиционным СМИ в последнее время постоянно снижается [*Николайчук, Янгляева, Якова* 2018], и наиболее социально активные граждане все чаще обращаются в поисках информации к альтернативным СМИ – социальным сетям и мессенджерам. Поэтому органам власти необходимо ориентироваться именно на эти источники информации, обеспечивая высокий уровень их информационной активности, поскольку, как пишет Х. Клинтон, «история показывает, что наилучшим ответом на порочащие высказывания является не их запрещение и блокировка, а подавление за счет преобладающего осуждения. Переводя проблему в плоскость дискуссий, правда будет только усиливаться, а слабые и ложные мнения и высказывания окажутся дискредитированы, пусть не сразу, но в конечном счете» [*Clinton* 2011].

Кибервойны как элемент гибридной войны

Кибербезопасность в условиях гибридной войны приобретает особую важность, поскольку сегодня уже практически невозможно представить себе ни один объект технологической инфраструктуры, который не был бы оснащен разного рода программными комплексами, многие из которых имеют выход в сеть Интернет, что несет серьезные риски. Так, компьютерная атака, направленная на важное инфра-

7 Так, в США широкую известность получил так называемый «Честный голос», находящийся в прямом подчинении Центрального командования Вооруженных сил (CENTCOM) [*Виловатых* 2018].

8 Технический прием создания в социальных сетях фейковых пользователей и их групп, направленный на продвижение (или высмеивание) определенных идей либо создание впечатления «массовости» поддержки определенных идей или требований.

9 Словосочетания или графические изображения, которые получают массовое распространение и наделяются определенным смыслом, например, флаг ЕС с гербом Украины в период Майдана или женщина в красном платье во время волнений в Турции.

структурное предприятие, может привести не только к полному прекращению или нарушению функционирования данного объекта, но и оказать более комплексное воздействие на экономику страны в целом, а также нести в себе серьезную угрозу безопасности граждан.

Кроме того, кибератаки могут быть использованы как вспомогательное средство в рамках информационной войны, с целью взлома закрытых данных и их опубликования либо «вброса» фейковой информации, в т. ч. со ссылкой на источники, внушающие доверие.

Все это заставляет по-новому смотреть на проблему кибербезопасности, особенно когда речь идет об опасных объектах либо системах обеспечения жизнедеятельности. Возможен весьма широкий спектр последствий негативного воздействия с помощью современных технологий на функционирование объектов инфраструктуры – от отдельных человеческих жертв (например, в результате воздействия на автоматизированную систему управления транспортной инфраструктуры, на систему управления электроснабжением и т. д.) до значительных разрушений (воздействие на автоматизированные системы управления гидро-, электро- и атомных станций, экологически опасных химических производств и т. п.) и нарушения функционирования всей инфраструктуры как экономической основы существования государства. Соответственно, злонамеренное использование ИКТ способно нанести ущерб, сравнимый с применением традиционного оружия, а в ряде случаев – с использованием оружия массового поражения [*Вильданов, Башкиров* (2) 2019].

Так, основной целью кибератак на автоматизированные системы управления технологическими процессами является вывод технологического процесса на критические (аварийные) режимы, когда значения критических переменных состояния выходят за эксплуатационные пределы и приводят к значительным ущербам и авариям. Одним из примеров такой атаки может служить применение компьютерного червя Stuxnet, поразившего в 2010 г. ядерные объекты Ирана. Stuxnet был ориентирован на выведение из строя турбогенератора путем скачкообразного изменения частоты вращения свыше допустимых эксплуатационных пределов. Из-за «человеческого фактора» Stuxnet поразил ряд компьютеров на АЭС «Бушер», но это не привело к аварии на станции, т. к. не были заражены компьютеры турбинного отделения [*Калашников, Сакрутина* 2018].

Американские спецслужбы накопили обширную статистику в области проведения кибератак на объекты национальной инфраструктуры, где, как оказалось, энергетический сектор является первоочередной целью для дезорганизации работы всей инфраструктуры и экономики страны. Так, ежегодно регистрируется от 18 до 20 тыс. попыток проникновения в информационные сети электростанций, что составляет в среднем 35% кибератак на все объекты национальной инфраструктуры [*Башкиров* 2019]. То есть объекты, обеспечивающие жизнь миллионов простых людей (объекты критической инфраструктуры), оказываются уязвимыми как никогда и для прямых кибератак, и для нападений через инсайдеров, которые преднамеренно или нет своими действиями способствуют преодолению вредоносными программами специально создаваемых «воздушных зазоров» и «демилитаризованных зон» либо иным способом нарушают созданные системы защиты от кибератак.

Защита критической инфраструктуры становится общей проблемой всех государств, что заставляет рассматривать кибероружие как элемент сдержи-

вания наравне с ядерным оружием, а на международном уровне поднимать вопрос о недопустимости и преступности кибератак на такие объекты. Однако на сегодня отсутствуют международно-правовые нормы, регулирующие межгосударственные отношения в информационном пространстве, а существующее международное право к проблематике информационной и кибербезопасности практически не применимо.

Во многом это связано с тем, что данная сфера оказалась крайне политизированной, учитывая столкновение интересов и противоречивые позиции США и других стран, обладающих наиболее существенным киберпотенциалом. Причиной «сложности» западные эксперты считают тесное переплетение разнообразных интересов (военных, экономических, социальных, дипломатических) различных государств [*Вильданов, Башкиров* (1) 2019].

До сих пор не удается прийти к согласию по принципиальным моментам, например, как следует реализовать на практике концепцию суверенитета в киберпространстве, право на самооборону и соответствующие меры противодействия. Традиционно все перечисленное было принято связывать с территорией, однако информационная среда функционирует вне связи с территорией или какими-либо материальными объектами. Поэтому, например, английские ученые Tsagourias N. и Buchan R. предлагают более не связывать суверенитет и юрисдикцию с территорией конкретного государства; по их мнению, государства обладают экстерриториальной юрисдикцией в отношении киберпространства [*Tsagourias, Buchan* 2015].

Именно такой подход был реализован в принятом в 2018 г. в США «Облачном акте» – законе, устанавливающем юрисдикцию страны в отношении данных, находящихся на серверах в иностранных государствах. Принятие этого закона связано со спором Microsoft Corp. v. United States Department of Justice, возникшем после того, как правоохранительные органы США потребовали от компании Майкрософт предоставить свободный доступ к данным электронной почты пользователей в любых частях планеты, независимо от того, находятся ли они под американской юрисдикцией или нет. Майкрософт отказалась это делать, ссылаясь на то, что часть данных хранится на серверах, расположенных в Дублине, т. е. на них распространяется суверенитет Ирландии. Верховный Суд США поддержал Майкрософт в силу того, что Закон 1986 г. «О конфиденциальности электронной связи» не распространялся на данные, находящиеся за пределами США. Практически сразу после вынесения данного судебного решения и был принят Облачный акт, предоставляющий доступ правоохранительным органам США к данным интернет-пользователей за рубежом, а также обязывающий провайдеров сохранять, осуществлять резервное копирование, раскрывать содержание беспроводной или электронной коммуникации, любую запись или иную информацию клиента, абонента провайдера, независимо от того, находится ли такая информация в пределах или за пределами Соединенных Штатов. Учитывая транснациональный характер крупнейших американских компаний, очевидно, что речь идет о расширении киберсуверенитета и юрисдикции США практически на весь мир. При этом данный закон устанавливает, что запрет передачи данных местным законодательством не может являться основанием для непредоставления запрашиваемых данных американским властям.

Данное понимание суверенитета и юрисдикции государства вступает в серьезное противоречие с подхо-

дом к этому вопросу РФ. Под юрисдикцию РФ попадают объекты информатизации и информационные системы, сайты в сети Интернет и сети связи, находящиеся на территории РФ. Иными словами, подход российского права сводится к установлению территориальных границ в отношении физически находящихся на территории государства оборудования, серверов (интернет-ресурсов), компьютеров, а также информации, доступ к которой осуществляется с данных устройств. Вопрос о распространении суверенитета и юрисдикции на информационные ресурсы, доступ к которым поддерживается оборудованием, находящемся вне территории страны, не ставится [*Терентьева* 2019].

Позиция российского законодателя в определенной степени обоснована, поскольку с точки зрения обеспечения кибербезопасности базовым принципом является именно территориальный фактор. То есть физическое расположение информационной инфраструктуры на определенной территории позволяет обеспечить полноценный контроль за нормальным ее функционированием, а значит, и контроль над киберпространством, что, в свою очередь, позволяет обезопасить государство от таких угроз, как кибератаки, киберпреступления, кибершпионаж и киберконфликт [*Joubert* 2010].

Однако следует отметить, что сегодня в мире существует всего 13 DNS-серверов (основных серверов), 10 из которых расположены в США, 2 – на территории ЕС, 1 – в Японии. И хотя за последние годы различные страны создают собственные сервера, основные информационные потоки идут через главный сервер, расположенный на территории США [*Разумов* 2017].

Таким образом, складывается ситуация, при которой Россия сознательно ограничивает свой киберсуверенитет привязкой к территориальному расположению информационной инфраструктуры, но в то же время основные информационные потоки так или иначе проходят через сервер Соединенных Штатов, которые, напротив, стремятся распространить свой киберсуверенитет на весь мир. В качестве примера негативных последствий такой ситуации можно привести платежную систему МИР, которая не смогла обезопасить российский финансовый сектор от санкционных мер, принимаемых Западом, поскольку все транзакции осуществляются компаниями, подчиняющимися иностранной юрисдикции [*Катасонов* 2019].

Очевидно, что такая ситуация подрывает информационную безопасность страны, учитывая усиление разведывательной деятельности иностранных государств в отношении РФ, а также нарастание угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности России [Доктрина информационной безопасности 2016].

Кроме того, в мире отсутствует единое понимание того, что из себя представляет критическая инфраструктура, что неизбежно ведет к различным подходам к ее защите. Так, в США критическая инфраструктура – «совокупность физических или виртуальных систем и средств, важных для государства в такой мере, что их вывод из строя или уничтожение могут привести к губительным последствиям в области обороны, экономики, здравоохранения и безопасности нации» [*Михалевич* 2019]. Таким образом, в состав критической инфраструктуры США входят 16 секторов: химия, энергетика и связь, опасные производства, ядерные реакторы, гидросооружения, системы водоснабжения, оборонно-промышленный

комплекс, опасные производства, аварийные службы, продовольственный сектор и сельское хозяйство, медицина и здравоохранение, информационные технологии, транспортные системы, системы утилизации отходов, финансовый и коммерческий сектора, а также функционирование государственных органов.

В ЕС критическая инфраструктура – это актив, система или ее часть, расположенные в государствах-членах, которые необходимы для поддержания жизненно важных функций общества, здравоохранения, обороны, безопасности, экономического и социального благополучия людей, нарушение или разрушение которых может иметь существенное влияние на выполнение указанных функций. Таким образом, критическая инфраструктура ЕС объединяет девять секторов: энергетику, транспорт, водоснабжение, здравоохранение, ИКТ, финансы и страхование, государственные и административные службы, питание и сельское хозяйство, медиа и культурные ценности [*Михалевич* 2019].

В Российской Федерации также принят ряд нормативных правовых актов, направленных на обеспечение безопасности критической инфраструктуры. Так, в 2016 г. была утверждена Доктрина информационной безопасности Российской Федерации, в июле 2017 г. принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», определяющий основные понятия в данной сфере и устанавливающий правовые механизмы обеспечения безопасности критической информационной инфраструктуры. В его развитие в 2017 г. также был утвержден Указ Президента Российской Федерации «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Указанные нормативные правовые акты регламентируют деятельность государственных органов власти по вопросам обнаружения, ликвидации и устранения последствий компьютерных атак, вводят в законодательство новые определения, такие как компьютерная атака, объекты критической информационной инфраструктуры, компьютерные инциденты, а также выделяют в отдельную группу инфраструктурные объекты Российской Федерации, представляющие особую важность (объекты критической информационной инфраструктуры). Однако основной акцент в них делается на информационной инфраструктуре.

Так, в соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации», критическая информационная инфраструктура – это «информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов».

Что касается непосредственно «критической инфраструктуры», то данный термин нормативно в Российской Федерации не закреплен и не определен, однако в Федеральном законе «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» содержатся два близких по сути понятия: «критически важный объект – это объект, нарушение или прекращение функционирования которого приведет к потере управления экономикой Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы субъекта Российской Фе-

дерации, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения» и «потенциально опасный объект – это объект, на котором расположены здания и сооружения повышенного уровня ответственности, либо объект, на котором возможно одновременное пребывание более пяти тысяч человек».

Что касается основных, наиболее чувствительных с точки зрения обеспечения безопасности, секторов, то они косвенно определены в статье 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: здравоохранение, наука, транспорт, связь, энергетика, банковская и финансовая сфера, топливно-энергетический комплекс, атомная энергетика, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность.

Таким образом, очевидна необходимость пересмотра и актуализации указанного законодательства с учетом развития технологий и анализа опыта других стран в вопросах защиты критической инфраструктуры. Важно также учитывать, что основой информационной и кибербезопасности является создание мощной информационной инфраструктуры и конкурентоспособных отечественных информационных технологий, а в России до сих пор сохраняется недопустимо высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий и их использования для производства продукции и оказания услуг, что обуславливает зависимость социально-экономического развития России от геополитических интересов зарубежных стран и, прежде всего, США [Доктрина информационной безопасности 2016].

Кроме того, обеспечить достаточно эффективную информационную и кибербезопасность возможно только выработкой коллективных межгосударственных стратегий государств-партнеров по интеграционным объединениям, т. е. посредством принятия мер коллективной безопасности, поэтому следует обратить особое внимание на усиление взаимодействия по данному направлению в рамках СНГ и ЕАЭС.

«Цветные революции» как элемент гибридной войны

Как отмечалось выше, политика «мягкой силы», проводимая в рамках гибридной войны, имеет своей целью разрушение традиционных ценностей и подмену их чужеродными псевдоценностями, формирование негативного отношения к существующему строю, органам власти, политическим лидерам. Конечная цель информационной войны – это манипулирование сознанием населения противника, приводящее к разрушению государства-противника руками его же собственного населения при поддержке мирового сообщества. Для этого используются «агенты влияния», «лидеры мнения» из местного населения, целью деятельности которых является организация протестных акций, провокаций власти и массовых мероприятий, дискредитирующих правительство.

В современных условиях основная активность таких «лидеров мнения» уходит в Сеть, а в офлайн выплескивается уже подготовленными акциями[10].

В связи с этим представляет интерес описание в книге Хиллари Клинтон то-

10 Флешмобы, акции протеста А. Навального и др.

го, как Госдепартамент США организовывал курсы для оппозиционеров в социальных сетях, где их обучали, как составлять карты митингов и разгона демонстраций в режиме реального времени, разрабатывались специальные программы и устройства, которые позволяют оппозиционерам при задержании подавать сигнал своим товарищам, одновременно удаляя из телефона все контакты [*Клинтон* 2016].

Все эти действия направлены на формирование атмосферы общественного недовольства, которая в конечном итоге должна выливаться в акции гражданского неповиновения, перерастающие в «цветные революции».

Как отмечает Х. Клинтон, задачей внешнеполитического ведомства является интеграция глобальной коммуникационной стратегии при постоянной готовности раздуть протестный потенциал, возникающий из-за нарастающих экономических проблем, до революционных антиправительственных выступлений [*Клинтон* 2016].

Таким образом, основная роль «лидеров оппозиции» – не сформулировать четкую и практически реализуемую программу действий, а провозгласить такую программу, которая будет привлекать в ряды оппозиции неудовлетворенных людей (причем это может быть как неудовлетворенность экономическими или социальными условиями жизни, так и невозможность реализовать свой творческий потенциал, личная неудовлетворенность жизнью и т. п.). Как отмечает Э. Хоффер, массовые движения позволяют канализировать эту неудовлетворенность, компенсировать ее ощущением собственной силы индивида, проявляемой в активных действиях. Вера в «священное дело» замещает утраченную уверенность людей в себе. Массовое движение дает участникам надежду и смысл существования [*Хоффер* 2017].

Следует признать, что из всего разнообразия приемов и способов ведения гибридной войны явление «цветных революций» наиболее изучено, поэтому мы не будем останавливаться на нем подробно. Отметим только, что «цветная революция» характеризуется целеустремленным и массированным использованием информационных технологий (информационной войной) с целью расшатывания политической ситуации в стране, формирования в народе массового недовольства властью, превращения его в толпу и манипулирования ею для нанесения таранного удара по этой самой власти. Цель «цветных революций» – государственный переворот, поэтому они достаточно четко ограничены во времени, что позволяет отнести их к одному из способов или технологий ведения гибридной войны [*Брычков и др.* 2019].

Соответственно, данная технология может быть эффективно реализована только в том государстве, которое уже «подготовлено» при помощи других способов ведения гибридной войны, где достаточно высок уровень недовольства граждан и политическая ситуация нестабильна. В государствах со стабильной политической системой данный метод не дает необходимых результатов, поэтому гибридная война в отношении таких государств ведется по стратегии «измора», т. е. с использованием иных способов: информационной войны, кибератак, постоянной эскалации напряженности у ее границ, поддержки террористов и сепаратистов внутри страны и др.

В связи с этим важным механизмом противодействия со стороны государства является постоянный мониторинг не просто социально-экономической ситуации в стране, а именно состояния удовлетворенности/неудовлетворенности населения, что можно доста-

точно эффективно реализовать при помощи современных ИКТ [*Виловатых* 2018], и оперативное принятие мер по смягчению возникающей неудовлетворенности, поскольку «самая лучшая почва для массового движения – это общество, где достаточно свободы, но нет смягчающих средств против неудовлетворенности» [*Хоффер* 2017].

Выводы

Проведенный выше анализ элементов гибридной войны позволяет прийти к заключению, что войну провоцирует не сила нападающего, а слабость объекта нападения. Чтобы свести к минимуму появление многих угроз безопасности страны, необходимо решать проблему уязвимостей во всех сферах и на всех уровнях жизни общества, т. е. нужно работать на опережение и не допускать угроз.

Но комплексность, многоаспектность и непредсказуемость угроз, особенно связанных с распространением информационных технологий, требует не просто обеспечения безопасности, а выработки, принятия и реализации системного подхода, перехода к концепции комплексной безопасности, в основе которой лежат не просто военные и технические приемы и средства, а комплекс мер предупреждения всех существующих гибридных угроз, а также непрерывная аналитика и превентивное выявление будущих. Следует признать, что Военная доктрина России (утв. Президентом РФ 25.12.2014) практически целиком посвящена проблематике предотвращения вооруженных конфликтов и противодействия им в случае возникновения; остальные аспекты безопасности, такие как информационная безопасность, подрыв духовных ценностей и необходимость патриотического воспитания молодежи, в ней упоминаются вскользь. Вместе с тем в военных доктринах стран НАТО продвижение идей демократии обозначено в качестве важнейшей задачи Вооруженных сил, поскольку в процессе организации обороны этих стран при определении баланса между духовной и материальной субстанциями предпочтение все больше отдается первой [*Брычков и др.* 2019]. Соответственно, задачи Вооруженных сил западных стран обусловлены, прежде всего, необходимостью распространения универсальных ценностей.

Таким образом, представляется актуальной реализация комплексного подхода к обеспечению национальной безопасности Российской Федерации в условиях гибридной войны, который должен включать следующие элементы:

1. Выработку политики «мягкой силы», основанной прежде всего на защите, сохранении и развитии традиционных духовных ценностей.
2. Возвращение к традиционной системе школьного образования, включающего духовное воспитание.
3. Повышение эффективности патриотического воспитания молодежи, прежде всего за счет развития социальных инициатив, общественных движений и объединений, цели которых совпадают с государственной политикой идентичности.
4. Формирование и/или повышение активности служб информационной безопасности, с основной ориентацией их внимания на сетевые СМИ и социальные сети.
5. Переход от стратегии реагирования на уже распространенную в СМИ и Интернете информацию к стратегии заполнения информационных пустот объективной и качественной информацией.

6. Создание собственного DNS-сервера, а также качественного отечественного программного обеспечения для решения проблемы кибербезопасности объектов критической инфраструктуры.
7. Изменение федерального законодательства в целях устранения противоречий в подходах к определению и правовому статусу «критической инфраструктуры», «критически важных объектов» и «потенциально опасных объектов».
8. Разработку и реализацию программ повышения грамотности сотрудников, работающих на критических объектах инфраструктуры, и населения страны в целом в вопросах кибербезопасности и кибергигиены.
9. Сотрудничество со странами ЕАЭС в создании общего безопасного информационного пространства и обеспечении общей кибербезопасности.
10. Обеспечение постоянного мониторинга состояния социально-экономической удовлетворенности общества; разработку и внедрение мер против неудовлетворенности граждан.

При этом следует еще раз подчеркнуть, что базовой составной частью комплексной национальной безопасности должна быть духовная безопасность, которая представляет собой такое «состояние социокультурной среды, при котором объединяются общественное сознание, духовные ценности, культура и обеспечиваются условия для духовного совершенствования и прогресса личности, общества и государства на основе национальной самобытности и сохранения духовной общности народа» [*Газгиреева, Бурняшева* 2011].

Будущие исследования

В настоящем исследовании не было уделено достаточного внимания таким способам ведения гибридной войны, как поддержка сепаратистских и террористических организаций, принятие мер, направленных на повышение уровня криминализации общества, экономическое порабощение противника и его элит, мерам экономического давления. Как отмечает М.Е. Кучинская, США уделяют повышенное внимание экономической составляющей в рамках ведущейся против РФ затяжной гибридной войны [*Кучинская* 2018]. Кроме того, ряд ученых сегодня предлагают относить к элементам гибридной войны искусственный интеллект и робототехнику [*Рогачев, Виловатых* 2019].

Следует признать, что тематика использования экономических методов, а также современных цифровых и сквозных технологий в качестве инструментов гибридной войны мало изучены в политологической литературе и требуют глубокого и системного исследования, что невозможно осуществить в рамках одной статьи. Таким образом, эти направления являются перспективными в дальнейших исследованиях феномена гибридности.

Заключение

Таким образом, сегодня в политической и военной доктрине многих стран все больше внимания уделяется гибридным способам межгосударственного противостояния, роль которых постоянно возрастает и которые с каждым годом становятся все сложнее и комплекснее. Это требует от России выработки «контргибридных» мер, основанных на обеспечении комплексной безопасности государства, базиру-

ющейся, прежде всего, не на противодействии существующим угрозам, а на определении и устранении собственных уязвимостей в тех сферах, где противники страны реализуют различные инструменты и способы ведения гибридной войны.

Список литературы

Башкиров Н. (2019) Обеспечение кибербезопасности электроэнергетической системы США // Зарубежное военное обозрение. № 3. С. 3–9. http://pentagonus.ru/publ/obespechenie_kiberbezopasnosti_ehlektroehnergeticheskoj_sistemy_ssha_2019/19-1-0-2889, дата обращения 20.05.2020.

Брычков А.С. и др. (2019) Гибридные войны XXI столетия: происхождение, сущность и место в цивилизационном процессе: Монография. Смоленск.

Виловатых А.В. (2018) Использование информационно-коммуникационных технологий в военно-политических целях: социально-психологический аспект // Проблемы национальной стратегии. № 2. С. 197–211 // https://riss.ru/images/pdf/journal/2018/2/09.pdf, дата обращения 20.05.2020.

Вильданов М., Башкиров Н. (1) (2019) Международно-правовые аспекты защиты инфраструктуры государств от киберугроз // Зарубежное военное обозрение. № 7. С. 3–10 // http://factmil.com/publ/soderzhanie/informacionnye_vojny/mezhdunarodno_pravovye_aspekty_zashhity_infrastruktury_gosudarstv_ot_kiberugroz_2019/107-1-0-1659, дата обращения 20.05.2020.

Вильданов М., Башкиров Н. (2) (2019) Международно-правовые аспекты защиты инфраструктуры государств от киберугроз // Зарубежное военное обозрение. № 8. С. 21–26 // http://factmil.com/publ/soderzhanie/informacionnye_vojny/mezhdunarodno_pravovye_aspekty_zashhity_infrastruktury_gosudarstv_ot_kiberugroz_2019/107-1-0-1659, дата обращения 20.05.2020.

Газгиреева Л.Х., Бурняшева Л.А. (2011) Экзистенциальные основы духовной безопасности российского общества // Власть. № 2. С. 11–15 // https://cyberleninka.ru/article/n/ekzistentsialnye-osnovy-duhovnoy-bezopasnosti-rossiyskogo-obschestva/viewer, дата обращения 20.05.2020.

Доктрина информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.16 г. № 646 (2016) // Консультант плюс // http://www.consultant.ru/document/cons_doc_LAW_208191/, дата обращения 20.05.2020.

Калашников А.О., Сакрутина Е.А. (2018) Прогнозирование рискового потенциала объектов критической инфраструктуры атомных электростанций // Управление развитием крупномасштабных систем. М.: Институт проблем управления им. В.А. Трапезникова РАН. С. 245–247 // https://elibrary.ru/item.asp?id=36620660, дата обращения 20.05.2020.

Катасонов В.Ю. (2019) «Китайский синдром» Путина. Прорыв или утопия? М.: Алгоритм.

Клинтон Х.Р. (2016) Тяжелые времена. М.: Эксмо.

Крячкина Ю.А. (2019) «Мягкая сила» во внешней политике Японии: ключевые особенности // Проблемы национальной стратегии. № 6. С. 95–107 // https://riss.ru/bookstore/journal/2019-g/problemy-natsionalnoj-strategii-6-57/, дата обращения 20.05.2020.

Кучинская М.Е. (2018) Феномен гибридизации современных конфликтов: отечественный и западный военно-политический дискурс // Проблемы национальной стратегии. № 6. С. 122–143 // https://riss.ru/bookstore/journal/2018-g/6-51/, дата обращения 20.05.2020.

Ладыгин Ф.И., Афанасьев С.В. (2017) Военно-доктринальный базис внешней политики США. М.: Кучково поле.

Михалевич И.Ф. (2019) Критические информационные инфраструктуры в контексте общей безопасности // Технологии информационного общества. М.: Медиа Паблишер. С. 370–372.

Николайчук И.А., Янгляева М.М., Якова Т.С. (2018) Крылья хаоса: Массмедиа, мировая политика и безопасность государства. М.: Икар.

О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.17 г. № 187-ФЗ (2017) // Консультант плюс // http://www.consultant.ru/document/cons_doc_LAW_220885/, дата обращения 20.05.2020.

О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера: Федеральный закон от 21.12.1994 № 68-ФЗ (1994) // Консультант плюс // http://www.consultant.ru/document/Cons_doc_LAW_5295/bb9e97fad-9d14ac66df4b6e67c453d1be3b77b4c/, дата обращения 20.05.2020.

Об утверждении Концепции внешней политики Российской Федерации: Указ Президента РФ от 30.11.2016 г. № 640 (2016) // Консультант плюс // http://www.consultant.ru/document/cons_doc_LAW_207990/, дата обращения 20.05.2020.

Панова А.В. (2019) Национальное сознание и правосознание в условиях информационной экономики. Владимир: АРКАИМ.

Политика «мягкой силы» Китая в Азии (аналитический доклад РИСИ) (2019) // Проблемы национальной стратегии. № 3. С. 11–67 // https://riss.ru/bookstore/journal/2019-g/3-54/, дата обращения 20.05.2020.

Разумов Е.А. (2017) Киберсуверенитет как аспект системы национальной безопасности КНР // Россия и Китай: история и перспективы сотрудничества. Материалы VII международной научно-практической конференции. С. 707–710 // https://elibrary.ru/item.asp?id=29191372, дата обращения 20.05.2020.

Рогачев С.В., Виловатых А.В. (2019) Информационное обеспечение внешнеполитической деятельности в условиях цифровой реальности // Проблемы национальной стратегии. № 6. С. 108–117 // https://riss.ru/bookstore/journal/2019-g/problemy-natsionalnoj-strategii-6-57/, дата обращения 20.05.2020.

Симагути М. (2006) Эпоха системных инноваций. М.: Миракл.

Ступаков Н.В. (2018) «Мягкая сила» как фактор, влияющий на результативность внешней политики в международных отношениях евразийских государств и построение стратегической платформы безопасности России, стран СНГ и ЕАЭС // Международное сотрудничество евразийских государств: политика, экономика, право. № 3. С. 24–37 // https://cyberleninka.ru/article/n/myagkaya-sila-kak-faktor-vliyayuschiy-na-rezultativnost-vneshney-politiki-v-mezhdunarodnyh-otnosheniyah-evraziyskih-gosudarstv-i/viewer, дата обращения 20.05.2020.

Сундиев И.Ю., Фролов А.Б. (2019) Наука в период «переквантования реальности и информационного-когнитивные механизмы социальной деструкции» // Экономические стратегии. № 5. С. 70–81. DOI: 10.33917/es-5.163.2019.70-81

Сургуладзе В.Ш. (2019) Политика идентичности в реалиях обеспечения национальной безопасности: Стратегия, теория, практика. М.: С.Т.К.

Терентьева Л.В. (2019) Территориальный аспект юрисдикции и суверенитета государства в киберпространстве // LEX RUSSICA (РУССКИЙ ЗАКОН). № 4(149). С. 139–150 // https://cyberleninka.ru/article/n/territorialnyy-aspekt-yurisdiktsii-i-suvereniteta-

gosudarstva-v-kiberprostranstve/viewer, дата обращения 20.05.2020.

Фриман Ч. (2018) Технологии, государственное управление и неограниченная война // Россия в глобальной политике. № 1 // http://www.globalaffairs.ru/number/Tekhnologii-gosudarstvennoe-upravlenie-i-neogranichennaya-voina-19349, дата обращения 20.05.2020.

Фролов А.В. (2019) Локальный конфликт: современный инструментарий // Ученые записки института Африки РАН. № 1(46). С. 17–35. DOI: 10.31132/2412-5717-2019-46-1-17-35

Хоффер Э. (2017) Человек убежденный: Личность, власть и массовые движения. М.: Альпина Паблишер.

Шукшин В.С., Суворов В.Л. (2017) Войны нового поколения: гибридная война – миф или реальность? М.: ИПО «У Никитских ворот».

Adams J., Albakajai M. (2016) Cyberspace: A New Threat to the Sovereignty of the State // Management Studies, vol. 4, no 6, pp. 256–265. DOI: 10.17265/2328-2185/2016.06.003

Bowman M. (2018) Senate Democrats Accuse Trump of Failing to Confront Russian Threat // VOA News, January 10, 2018 // https://www.voanews.com/usa/senate-democrats-accuse-trump-failing-confront-russian-threat, дата обращения 20.05.2020.

Breden J. (2013) Intell Tool Would Track Social Media like a Virus // GCN Magazine, February 12, 2013 // https://gcn.com/articles/2013/02/12/intell-tool-track-social-media-like-a-virus.aspx, дата обращения 20.05.2020.

Calpbinici P., Arslan F.T. (2019) Virtual Behaviors Affecting Adolescent Mental Health: The Usage of Internet and Mobile Phone and Cyberbullying // Journal of Child and Adolescent Psychiatric Nursing, vol. 32, no 3, pp. 139–148. DOI: 10.1111/jcap.12244

Clas A.M. (2018) Commanding in Multi-Domain Formations // Military Review. March–April // https://www.questia.com/library/journal/1G1-536534305/commanding-in-multi-domain-formations, дата обращения 20.05.2020.

Clinton H. (2011) Internet Rights and Wrongs: Choices & Challenges in a Networked World // U.S. Department of State, February 15, 2011 // https://2009-2017.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm, дата обращения 20.05.2020.

Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces (2019) // MCDC // https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840513/20190401-MCDC_CHW_Information_note_-_Conceptual_Foundations.pdf, дата обращения 20.05.2020.

Ford Ch.M., Williams W.S. (2018) Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare, Oxford University Press.

Hoffman F. (2009) Hybrid Warfare and Challenges // Joint Force Quarterly, no 52, pp. 34–39 // https://smallwarsjournal.com/documents/jfqhoffman.pdf, дата обращения 20.05.2020.

Hunter E., Pernik P. (2015) The Challenges of Hybrid Warfare, Tallinn: International Centre for Defence and Security // https://icds.ee/wp-content/uploads/2013/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf, дата обращения 20.05.2020.

Johnson D.R. (1996) Law and Borders: The Rise of Law in Cyberspace // Stanford Law Review, vol. 46, p. 1367. DOI: 10.2139/ssrn.535

Joubert V. (2010) Getting the Essence of Cyberspace: A Theoretical Framework to Face Cyber // Conference on Cyber Conflict Proceedings, Tallinn // https://ccdcoe.org/uploads/2018/10/Joubert-Getting-the-Essence-of-Cyberspace.pdf, дата обращения 20.05.2020.

Karlsen G.H. (2019) Divide and Rule: Ten Lessons about Russian Political In-

fluence Activities in Europe // Palgrave Communications, vol. 5, no 19, pp. 1–14. DOI: 10.1057/s41599-019-0227-8

Major J.R., Davis Jr. (2015) Continued Evolution of Hybrid Threats: The Russian Hybrid Threat Construct and the Need for Innovation // The Three Swords Magazine. No. 28.

Matusitz J. (2014) Intercultural Perspectives on Cyberspace: An Updated Examination // Journal of Human Behaviour in the Social Environment, vol. 24, no 7, pp. 713–724. DOI: 10.1080/10911359.2013.849223

Song M., Zhu Zh., Liu Sh., Fan H., Zhu T., Zhang L. (2019) Effects of Aggressive Traits on Cyberbullying: Mediated Moderation or Moderated Mediation? // Computers in Human Behavior, vol. 97, pp. 167–178. DOI: 10.1016/j.chb.2019.03.015

The Secretary General's Annual Report (2017) // NATO // https://www.nato.int/cps/en/natohq/opinions_152797.htm, дата обращения 20.05.2020.

The Soft Power 30 (2019) // https://softpower30.com/wp-content/uploads/2019/10/The-Soft-Power-30-Report-2019-1.pdf, дата обращения 20.05.2020.

Tsagourias N., Buchan R. (eds.) (2015) Research Handbook on International Law and Cyberspace, Sheffield: Edward Elgar Publishing.

Williamson M., Mansoor P.R. (2012) Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present, Cambridge: Cambridge University Press.

Yuchang J., Junyi L., Junxiu A., Jing W., Mingcheng H. (2019) The Differential Victimization Associated with Depression and Anxiety in Cross-cultural Perspective: A Meta-analysis // Trauma, Violence & Abuse, vol. 20, no 4, pp. 560–573. DOI: 10.1177/1524838017726426

Russian Experience

DOI: 10.23932/2542-0240-2020-13-2-3

"Hybrid Threats" to Russia's Security: Identification and Counteraction

Svetlana I. KODANEVA
PhD in Law, Senior Researcher
Institute of Scientific Information on Social Sciences (INION) of the Russian Academy of Sciences, 117218, Krzhizhanovskij St., 15-2, Moscow, Russian Federation
E-mail: kodanevas@gmail.com
ORCID: 0000-0002-8232-9533

CITATION: Kodaneva S.I. (2020) "Hybrid Threats" to Russia's Security: Identification and Counteraction. *Outlines of Global Transformations: Politics, Economics, Law*, vol. 13, no 2, pp. 44–71 (in Russian). DOI: 10.23932/2542-0240-2020-13-2-3

Received: 25.01.2020.

ABSTRACT. *In the scientific literature, it is customary to consider and analyze war exclusively as a violent (conventional) confrontation of subjects of international politics. However, this does not take into account that modern wars are increasingly unfolding in the "grey zone", that is, outside the framework of international law, they are conducted both in physical and in other dimensions – informational, cybernetic, cultural, cognitive – and mainly by non-military means and with the involvement of irregular formations (rebels, terrorists, etc.). As a result, today's interstate confrontation is becoming more complex and hybrid, presenting new mechanisms for non-nuclear deterrence.*

It is important to understand that the inability to recognize the enemy's ongoing war in time, to determine the direction of the strike destroyed many states, starting with the Roman Empire and ending with the USSR. This determines the relevance and timeliness of this study, which is aimed at analyzing the content of the phenomenon of hybrid war, determining the main methods of its conduct used today and proposing counteraction measures.

It should be recognized that in the modern scientific literature there is no single approach to understanding what a hybrid war is, which is quite understandable precisely because of its essence – the variability and complexity of ways of it conducting, as well as flexibility and adaptability to specific circumstances. There are quite a lot of disparate studies on individual components of hybrid war, such as "soft power", information, economic and cyberwar, "color revolutions", etc.

The subject of this research is the phenomenon of hybrid warfare, its content and specific ways of conducting hybrid warfare. The purpose of this work is to conduct a comprehensive analysis of the subject of research, as well as to structure the manifestation that form the phenomenon of hybrid war in its complex, determine their correlation and mutual influence of various methods of conducting hybrid war, as well as to develop specific proposals for countering threats to Russia's national security.

The importance of developing comprehensive strategic approaches aimed primarily at identifying vulnerabilities, as well as

including spiritual security as the basis of the entire security system and countering hybrid threats is emphasized.

Taking into account the specified subject and purpose, the introduction reveals the relevance of the study of the phenomenon of hybrid war and the danger that this type of interstate confrontation poses for Russia. Then we analyze the concept of hybrid war and its content, as well as the four main ways of conducting it. The results of the analysis are followed by conclusions and proposals on countering threats to Russia's national security.

KEY WORDS: *hybrid warfare, hybrid threats, soft power, information warfare, information security, cybersecurity, social networks, critical infrastructure, national security*

References

About Protection of the Population and Territories from Emergency Situations of Natural and Technogenic Character: Federal Law at 21.12.1994, No. 68-FZ (1994). *Consultant plus.* Available at: http://www.consultant.ru/document/Cons_doc_LAW_5295/bb9e97fad9d14ac66df4b6e67c453d1be3b77b4c/, accessed 20.05.2020 (in Russian).

Adams J., Albakajai M. (2016) Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies,* vol. 4, no 6, pp. 256–265. DOI: 10.17265/2328-2185/2016.06.003

Bashkirov N. (2019) Ensuring Cybersecurity of the US Electric Power System. *Foreign Military Review,* no 3, pp. 3–9. Available at: http://pentagonus.ru/publ/obespechenie_kiberbezopasnosti_ehlektroehnergeticheskoj_sistemy_ssha_2019/19-1-0-2889, accessed 20.05.2020 (in Russian).

Bowman M. (2018) Senate Democrats Accuse Trump of Failing to Confront Russian Threat. *VOA News,* January 10, 2018. Available at: https://www.voanews.com/usa/senate-democrats-accuse-trump-failing-confront-russian-threat, accessed 20.05.2020.

Breden J. (2013) Intell Tool Would Track Social Media like a Virus. *GCN Magazine,* February 12, 2013. Available at: https://gcn.com/articles/2013/02/12/intell-tool-track-social-media-like-a-virus.aspx, accessed 20.05.2020.

Brychkov A.S. et al. (2019) *Hybrid Wars of the XXI Century: Origin, Essence and Place in the Civilizational Process: Monograph*, Smolensk (in Russian).

Calpbinici P., Arslan F.T. (2019) Virtual Behaviors Affecting Adolescent Mental Health: The Usage of Internet and Mobile Phone and Cyberbullying. *Journal of Child and Adolescent Psychiatric Nursing,* vol. 32, no 3, pp. 139–148. DOI: 10.1111/jcap.12244

China's Soft Power Policy in Asia (RISS Report) (2019). *Problems of National Strategy*, no 3, pp. 11–67. Available at: https://riss.ru/bookstore/journal/2019-g/3-54/, accessed 20.05.2020 (in Russian).

Clas A.M. (2018) Commanding in Multi-Domain Formations. *Military Review.* March–April. Available at: https://www.questia.com/library/journal/1G1-536534305/commanding-in-multi-domain-formations, accessed 20.05.2020.

Clinton H. (2011) Internet Rights and Wrongs: Choices & Challenges in a Networked World. *U.S. Department of State*, February 15, 2011. Available at: https://2009-2017.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm, accessed 20.05.2020.

Clinton H.R. (2016) *Hard Choices,* Moscow: Eksmo (in Russian).

Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces (2019). *MCDC.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840513/20190401-

MCDC_CHW_Information_note_-_Conceptual_Foundations.pdf, accessed 20.05.2020.

Ford Ch.M., Williams W.S. (2018) *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare,* Oxford University Press.

Friman Ch. (2018) Technology, Government, and Unlimited War. *Russia in Global Politics,* no 1. Available at: http://www.globalaffairs.ru/number/Tekhnologii-gosudarstvennoe-upravlenie-i-neogranichennaya-voina-19349, accessed 20.05.2020 (in Russian).

Frolov A.V. (2019) Local Conflict: Modern Tools. *Scientific Notes of the Institute of Africa RAS*, no 1(46), pp. 17–35 (in Russian). DOI: 10.31132/2412-5717-2019-46-1-17-35

Gazgireeva L.H., Burnyasheva L.A. (2011) Existential Foundations of Spiritual Security of Russian Society. *Power,* no 2, pp. 11–15. Available at: https://cyberleninka.ru/article/n/ekzistentsialnye-osnovy-duhovnoy-bezopasnosti-rossiyskogo-obschestva/viewer, accessed 20.05.2020 (in Russian).

Hoffer E. (2017) *The Convinced Man: Personality, Power, and Mass Movements,* Moscow: Alpina Publisher (in Russian).

Hoffman F. (2009) Hybrid Warfare and Challenges. *Joint Force Quarterly*, no 52, pp. 34–39. Available at: https://smallwarsjournal.com/documents/jfqhoffman.pdf, accessed 20.05.2020.

Hunter E., Pernik P. (2015) *The Challenges of Hybrid Warfare*, Tallinn: International Centre for Defence and Security. Available at: https://icds.ee/wp-content/uploads/2013/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf, accessed 20.05.2020.

Information Security Doctrine of the Russian Federation: Decree of the President of the Russian Federation at 05.12.16 r. № 646 (2016). *Consultant plus*. Available at: http://www.consultant.ru/document/cons_doc_LAW_208191/, accessed 20.05.2020 (in Russian).

Johnson D.R. (1996) Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, vol. 46, p. 1367. DOI: 10.2139/ssrn.535

Joubert V. (2010) Getting the Essence of Cyberspace: A Theoretical Framework to Face Cyber. *Conference on Cyber Conflict Proceeding,* Tallinn. Available at: https://ccdcoe.org/uploads/2018/10/Joubert-Getting-the-Essence-of-Cyberspace.pdf, accessed 20.05.2020.

Kalashnikov A.O., Sakrutina E.A. (2018) Forecasting the Risk Potential of Critical Infrastructure Objects in Nuclear Power Plants. *Managing the Development of Large-scale Systems*, Moscow: Institute of management problems of the Russian Academy of Sciences, pp. 245–247. Available at: https://elibrary.ru/item.asp?id=36620660, accessed 20.05.2020 (in Russian).

Karlsen G.H. (2019) Divide and Rule: Ten Lessons about Russian Political Influence Activities in Europe. *Palgrave Communications,* vol. 5, no 19, pp. 1–14. DOI: 10.1057/s41599-019-0227-8

Katasonov V.Yu. (2019) *"Chinese Syndrome" of Putin. Breakthrough or Utopia?* Moscow: Algoritm (in Russian).

Kryachkina J.A. (2019) Key Features of Applying Japan's Soft Power to Its Foreign Policy. *Problems of National Strategy,* no 6, pp. 95–107. Available at: https://riss.ru/bookstore/journal/2019-g/problemy-natsionalnoj-strategii-6-57/, accessed 20.05.2020 (in Russian).

Kuchinskaya M. E. (2018) The Phenomenon of Hybridization of Modern Conflicts: Domestic and Western Military-political Discourse. *Problems of National Strategy*, no 6, pp. 122–143. Available at: https://riss.ru/bookstore/journal/2018-g/6-51/, accessed 20.05.2020 (in Russian).

Ladygin F.I., Afanasyev S.V. (2017) *Military Doctrinal Basis of US Foreign Policy*, Moscow: Kuchkovo pole (in Russian).

Major J.R., Davis Jr. (2015) Continued Evolution of Hybrid Threats: The Russian

Hybrid Threat Construct and the Need for Innovation. *The Three Swords Magazine*. No. 28.

Matusitz J. (2014) Intercultural Perspectives on Cyberspace: An Updated Examination. *Journal of Human Behaviour in the Social Environment*, vol. 24, no 7, pp. 713–724. DOI: 10.1080/10911359.2013.849223

Mikhalevich I.F. (2019) Critical Information Infrastructures in the Context of General Security. *Information Society Technologies*, Moscow: Media Publisher, pp. 370–372 (in Russian).

Nikolaichuk I.A., Yanklyaeva M.M., Yakova T.S. (2018) *Wings of Chaos: Mass Media, World Politics and State Security*, Moscow: Icarus (in Russian).

On Approval of the Concept of Foreign Policy of the Russian Federation: Decree of the President of the Russian Federation at 30.11.2016, No. 640 (2016). *Consultant plus*. Available at: http://www.consultant.ru/document/cons_doc_LAW_207990/, accessed 20.05.2020 (in Russian).

On Security of Critical Information Infrastructure of the Russian Federation: Federal Law at 26.07.17, No. 187-FZ (2017). *Consultant plus*. Available at: http://www.consultant.ru/document/cons_doc_LAW_220885/, accessed 20.05.2020 (in Russian).

Panova A.V. (2019) *National Consciousness and Legal Awareness in the Information Economy,* Vladimir: ARKAIM (in Russian).

Razumov E. A. (2017) Cyber Sovereignty as an Aspect of the National Security System of the PRC. *Russia and China: History and Prospects of Cooperation. Materials of the VII International Scientific and Practical Conference*, pp. 707–710. Available at: https://elibrary.ru/item.asp?id=29191372, accessed 20.05.2020 (in Russian).

Rogachev S.V., Vilovatykh A.V. (2019) Information Support of Foreign-Policy Activities in the Age of Digital Reality. *Problems of National Strategy,* no 6, pp. 108–117. Available at: https://riss.ru/bookstore/journal/2019-g/problemy-natsionalnoj-strategii-6-57/, accessed 20.05.2020 (in Russian).

Shimaguchi M. (2006) *Epoch of System Innovations,* Moscow: Miracl (in Russian).

Shukshin V.S., Suvorov V.L. (2017) *New Generation Wars: Hybrid Warfare – Myth or Reality?* Moscow: U Nikitskih vorot (in Russian).

Song M., Zhu Zh., Liu Sh., Fan H., Zhu T., Zhang L. (2019) Effects of Aggressive Traits on Cyberbullying: Mediated Moderation or Moderated Mediation? *Computers in Human Behavior*, vol. 97, pp. 167–178. DOI: 10.1016/j.chb.2019.03.015

Stupakov N.V. (2018) "Soft Power" as a Factor Influencing the Effectiveness of Foreign Policy in International Relations of Eurasian States and Building a Strategic Security Platform for Russia, the CIS Countries and the EAEU. *International Cooperation of the Eurasian States: Politics, Economics, Law*, no 3, pp. 24–37. Available at: https://cyberleninka.ru/article/n/myagkaya-sila-kak-faktor-vliyayuschiy-narezultativnost-vneshney-politiki-v-mezhdunarodnyh-otnosheniyah-evraziyskih-gosudarstv-i/viewer, accessed 20.05.2020 (in Russian).

Sundiev I.Yu., Frolov A.B. (2019) Science Is in a Period of "Perekantovatsya Reality and Information-cognitive Mechanisms of Social Destruction". *Economic Strategy*, no 5, pp. 70–81 (in Russian). DOI: 10.33917/es-5.163.2019.70-81

Surguladze V.Sh. (2019) *Identity Politics in the Realities of Ensuring National Security: Strategy, Theory, Practice*, Moscow: Analytical group «S.T.K.» (in Russian).

Terentyeva L.V. (2019) Territorial Aspect of State Jurisdiction and Sovereignty in Cyberspace. *LEX RUSSICA (RUSSIAN LAW)*, no 4(149), pp. 139–150. Available at: https://cyberleninka.ru/article/n/territorialnyy-aspekt-yurisdiktsii-i-suvereniteta-gosudarstva-v-kiberprostranstve/viewer, accessed 20.05.2020 (in Russian).

The Secretary General's Annual Report (2017). *NATO*. Available at: https://www.nato.int/cps/en/natohq/opinions_152797.htm, accessed 20.05.2020.

The Soft Power 30 (2019). Available at: https://softpower30.com/wp-content/uploads/2019/10/The-Soft-Power-30-Report-2019-1.pdf, accessed 20.05.2020.

Tsagourias N., Buchan R. (eds.) (2015) *Research Handbook on International Law and Cyberspace*, Sheffield: Edward Elgar Publishing.

Vildanov M., Bashkirov N. (1) (2019) International Legal Aspects of Protecting the Infrastructure of States from Cyber Threats. *Foreign Military Review,* no 7, pp. 3–10. Available at: http://factmil.com/publ/soderzhanie/informacionnye_vojny/mezhdunarodno_pravovye_aspekty_zashhity_infrastruktury_gosudarstv_ot_kiberugroz_2019/107-1-0-1659, accessed 20.05.2020 (in Russian).

Vildanov M., Bashkirov N. (2) (2019) International Legal Aspects of Protecting the Infrastructure of States from Cyber Threats. *Foreign Military Review*, no 8, pp. 21–26. Available at: http://factmil.com/publ/soderzhanie/informacionnye_vojny/mezhdunarodno_pravovye_aspekty_zashhity_infrastruktury_gosudarstv_ot_kiberugroz_2019/107-1-0-1659, accessed 20.05.2020 (in Russian).

Vilovatykh A.V. (2018) Information & Communication Technologies on the Political-Military Service: the Social and Psychological Aspects. *Problems of National Strategy*, no 2, pp. 197–211. Available at: https://riss.ru/images/pdf/journal/2018/2/09.pdf, accessed 20.05.2020 (in Russian).

Williamson M., Mansoor P.R. (2012) *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge: Cambridge University Press.

Yuchang J., Junyi L., Junxiu A., Jing W., Mingcheng H. (2019) The Differential Victimization Associated with Depression and Anxiety in Cross-cultural Perspective: A Meta-analysis. *Trauma, Violence & Abuse*, vol. 20, no 4, pp. 560–573. DOI: 10.1177/1524838017726426