Для решения задач информационно-психологического воздействия на политически активную часть населения Российской Федерации спецслужбами США на территории стран НАТО, прилегающих к западным границам России создана взаимосвязанная мощная организационно-технологическая система информационной войны на российском направлении.

Первый этап использования этого инструментария осуществлен в августе 2008 года при вооруженном нападении Грузии на Южную Осетию. Заранее подготовленная и срежиссированная информационно-пропагандистская кампания Запада в поддержку Тбилиси была направлена на формирование у международного общественного мнения образа агрессора в лице России.

Для полноты понимания задействованных в

информационной войне ресурсов объемы финансирования развития отдельных направлений информационных и коммуникационных технологий, разведывательных информационных технологий, научно-исследовательские работы и информационные операции, предусмотренные законами о национальной обороне США, с 2016 по 2021 год было выделено из бюджета Пентагона до 1 миллиарда 390 миллионов долларов. Примеров тенденциозных агрессивных информационных кампаний и кибератак наших оппонентов для раскручивания инцидентов в информпространстве можно привести множество.

Условно их разделим на несколько крупных целевых групп в интересах:
– демонизации России, дестабилизации общества и смены государственной власти;
– продвижения США и их сателлитами экономических интересов, включая доступ к российским природным ресурсам, на условиях, отвечающих потребностям транснациональных компаний;
– обоснования ухудшения внутриполитической и социально-экономической ситуации в странах западной демократии «разнообразной злонамеренной и вредоносной деятельностью» Российской Федерации;
– нанесения ущерба национальным интересам России в различных областях.

В национальной Стратегии кибербезопасности США определили четыре основных направления.
Их классификация закамуфлирована следующим образом: защита национальной инфраструктуры и людей, развитие цифровой экономики, сохранение мира и спокойствия, укрепление американского влияния.

Из последних подобных акций можно отметить:
– выдвижение в адрес России бездоказательных обвинений в кибератаках на государственные органы и СМИ Грузии в

октябре 2019 года;
– поднятую шумиху в СМИ о «бесчеловечных» атаках на объекты здравоохранения Чехии, задействованные в борьбе с коронавирусом;
– вброс заявлений об обнаружении попыток «русских хакеров» получить доступ к сетям разработчиков вакцины от COVID-19 из США, Великобритании и Канады.

В октябре 2020 года в США обвинили хакерскую группу Sandworm, созданную якобы из сотрудников ГРУ ГШ, в распространении вируса NotPetya, не принимая во внимание нанесение вирусом ущерба не только компаниям и госорганам США, Европы, Индии, Китая, Австралии, но и «Роснефти» и «Башнефти» в РФ.
Отдельного внимания заслуживает долгоиграющая тема так называемого российского влияния на результаты выборов в США, в частности с использованием информационных технологий. Политизация американскими властями с привлечением спецслужб, СМИ и НПО придуманного обвинения Кремля в зловредном воздействии на выборные процессы в Штатах вывела проблему за рамки дипломатического диалога. Впоследствии по указанию президента США началась скрытая кибератака на российское Агентство интернет-исследований, которое было без предъявления доказательств названо штатовскими спецслужбами распространителем дезинформации, квалифицируемой как вмешательство. Факт этой атаки экс-президент США Дональд Трамп признал публично.

Кроме того, эта надуманная причина послужила основанием для главы Белого дома наделить в 2018 году ЦРУ расширенными полномочиями при осуществлении наступательных операций в киберпространстве, включая вывод из строя инфраструктуры противника. Минюст США в отчете за 2021 финансовый год обвинил Россию, КНР, Иран и

КНДР в кибератаках на американские разработки вакцин от коронавируса с целью компрометации штатовских сетей и цепочек поставок, кражи интеллектуальной собственности, а также разжигания розни и подрыва демократии.

По примеру США Москве следует предъявить претензии Вашингтону за проведенную в ноябре 2021 года рекордную по мощности кибератаку на портал «Госуслуги», за ежедневные кибернападения с террористическими угрозами в адрес учебных заведений и торговых комплексов. Все они в основном идут с территории Украины, где криминальные ульи хакеров подготовлены натовскими специалистами.
Свежим ярким примером дезинформационной кампании является распространение разведслужбами США и Великобритании так называемых разведданных среди европейских союзников «о готовящемся вторжении российских войск на Украину». Вашингтон начал делиться «весьма подробной» информацией в начале ноября 2021 года перед встречей министров иностранных дел стран – членов НАТО, что помогло заручиться поддержкой Европы и главное – скептически настроенной Германии в сдерживании России. Одна наспех нарисованная карта с красными стрелами из России и Белоруссии стоила того, чтобы Берлин заявил 16 ноября о приостановке процесса сертификации компании Nord Stream 2 AG в качестве оператора нового российского газопровода. А игры поляков вокруг мигрантов на границе с Белоруссией способствовали созданию благоприятной атмосферы для обсуждения главами МИД стран блока на встрече 1 декабря 2021 года в Риге возможных экономических санкций против РФ.

Кроме того, на фоне раздутого миграционного кризиса в восточноевропейском регионе НАТО удалось убедить в необходимости расширения партнерства с Евросоюзом за счет финансирования европейцами кибернетической обороны

и мер по реагированию на гибридные угрозы.
По расчетам американцев, проведение данной кампании усилили переговорные позиции президента США в ходе российско-американского саммита по вопросу Украины и продвижения НАТО к границам России.

Для дезинформационных кампаний характерны несколько шаблонных признаков: – массовое распространение однотипной или идентичной информации с использованием СМИ и ИКТ; – многократное дублирование материала по различным каналам с привлечением для достоверности так называемых авторитетных личностей; – дискредитация источников альтернативных мнений и суждений на распространение ложной (фейковой) информации.
Комплексный анализ различных исследований и отчетов зарубежных и российских компаний в сфере информационной безопасности показывает, что наибольшее число компьютерных атак осуществляется с использованием инфраструктуры, расположенной в США.
Например, количество кибератак на критически важные объекты промышленности в 2020-м году увеличилось более чем в два раза по сравнению с 2019 годом. По заявлению президента Российской Федерации, за последние шесть лет число преступлений в ИТ-сфере выросло в 10 раз. По данным МВД России, в 2021 году четверть всех преступлений совершена с использованием IT-технологий. Потери мировой экономики от кибератак составили более 2,5 триллиона долларов (180 триллионов рублей), а по прогнозу на 2022 год достигнут 8 триллионов долларов. Причем американские хакеры с 2016 года в статистике вредоносной активности занимают лидирующее положение – от 40 до 75 процентов в зависимости от типа воздействий.
Для сравнения: России указанный показатель отводит до семи процентов, что подтверждает лживость тезиса о

тотальной российской угрозе в мировом информационном пространстве. Вместо совместной работы экспертов над выявлением, поиском истинных источников компьютерных атак и их нейтрализации, судебного наказания виновных, прежде всего в международно-правовом поле, США навязывают общественно-политическим кругам и правительствам механизм их определения (атрибуции) «с позиции консенсуса» (по согласию). То есть виновный может назначаться таковым в результате решения группы государств без предъявления каких-либо доказательств, а лишь на основании «компетентного» мнения стороны обвинения.

Особую актуальность данная тенденция приобретает в свете проведенного по инициативе Вашингтона 9–10 декабря 2021 года так называемого виртуального «саммита за демократию», в ходе которого участникам форума американцы настойчиво рекомендовали войти в «Альянс за будущее глобального Интернета» под предлогом необходимости создания механизма противодействия авторитарным державам осуществлять государственный контроль за деятельностью в сети Интернет.

После его проведения без участия постоянных членов СБ ООН Китая и России в 2022 году следует ожидать глубочайшего раскола мирового сообщества на два лагеря, роста напряженности в сфере информационного противоборства, негативно влияющей на состояние международной информбезопасности и стратегической стабильности в целом. Серьезность намерений США на этом направлении подтверждается активной деятельностью Запада по созданию Всемирной организации по цифровым данным (ВОЦД). Кукловоды и режиссеры из США твердо верят в реальность задуманного. Ранее в ООН и в мире проглотили ложь в отношении обоснованности применения военной силы в Ираке и Югославии, почему бы и в этом случае не использовать этот шаблон.

Таким образом, если называть вещи своими именами, дезинформационные кампании стали способом обоснования понятия «права на войну» (jus ad bellum), стирая различия с понятием «права войны» (jus in bello). А такой подход уже заложен в проекте Руководства по международному праву, применимому к кибернетическим способам ведения войны (или «Таллинском руководстве» 3.0.).

Следует заметить, что это тоже существенный пример постепенной подмены международного права так называемыми правилами демократического Запада (возврат «права силы» вместо «силы права»). Само понятие «права на войну» (jus ad bellum) противоречит основополагающим и признанным предыдущими поколениями принципам и нормам международного права, а также Уставу ООН, призывающему избавить будущие поколения от бедствий войны. Таким образом, стремление Штатов под влиянием транснациональных компаний и IT-гигантов монополизировать информационное пространство несет огромный конфликтный потенциал, вызывая сопротивление человечества. Для государств это потенциальная угроза утери суверенитета, а также присущих каждому народу традиционных культурно-нравственных ценностей.

Первоочередными мерами на национальном уровне следует считать совершенствование системы мониторинга и комплексной оценки информационной обстановки на основе повышения уровня координации и взаимодействия органов власти в рамках возложенных функций.

Важное значение имеет интенсификация процесса сбора, обработки и анализа громадных массивов информации за счет создания и развития программно-аппаратных комплексов с элементами искусственного интеллекта с использованием соответствующих регламентов.

Решение проблемы будет успешным в случае всеобъемлющего подхода, что требует совершенствования

системы стратегического планирования с учетом прогноза вызовов и угроз.

На глобальном уровне в настоящее время и на перспективу сохраняет свою актуальность широкий перечень возможных мер совершенствования существующей системы международного права для обеспечения международной информационной безопасности (МИБ), разработанный экспертами российской делегации по обеспечению деятельности Группы правительственных экспертов в Первом комитете Генеральной Ассамблеи ООН по проблеме МИБ. Эти усилия могут быть эффективно дополнены мерами обеспечения безопасности трансграничного обмена информацией с ограниченным доступом, интернационализацией управлением Интернетом, созданием международной системы мониторинга информационной обстановки.

Сергей КОРОТКОВ, кандидат военных наук