ВВЕДЕНИЕ

С момента начала интенсивного развития цифровых технологий жизнь человека перестала ограничиваться только физическим пространством. Всемирная сеть дала людям возможность искать информацию, производить контент и обмениваться им, а также пользоваться различными сервисами.

Пандемия коронавируса, начавшаяся в конце 2019 г., усилила эти тенденции и перевела значительную часть офлайн-активности в интернет: сегодня с его помощью люди гораздо чаще стали заказывать продукты и готовую еду домой, консультироваться с врачами, совершать денежные операции, проводить рабочие встречи и обучаться. Еще десять лет назад «умный дом» и искусственный интеллект звучали фантастично, а сегодня являются неотъемлемым направлением развития любой большой ИТ-компании.

Интернет уже давно является главным источником информации, оставив другие каналы — телевидение, пресса, радио — далеко позади. Появление и распространение смартфонов и других портативных устройств с выходом в глобальную паутину, а также развитие социальных сетей и модернизация СМИ привели к тому, что производство и потребление контента жителями почти всех стран мира выросло в сотни раз. Более того, перспективные и амбициозные проекты частных компаний по созданию общедоступных сетей Wi-Fi в ближайшем будущем, вероятно, обеспечат все человечество выходом в Сеть.

Формирование информационного (кибернетического) пространства не могло остаться незамеченным в сфере политики и военного дела. Если распространение печатных СМИ и радиовещания в конце XIX — начале XX в. привело к появлению концепции «психологической войны», то в 70-х гг. XX в. прогресс в сфере электроники породил идею войны информационной.

Данные концепции, непрерывно обновлявшиеся и развивающиеся с момента возникновения, постепенно эволюционировали до самостоятельного инструмента внешней политики в виде информационных и кибернетических операций (кибероперациий). Подробно этот путь проанализирован в первой части книги, разбитой для удобства читателя на три главы.

Первая глава представляет собой краткий исторический анализ использования различных инструментов пропаганды и иных форм психологического воздействия. В качестве точки отсчета взята Первая Мировая война (ведь именно в годы Великой войны впервые широко применялись инструменты психологического воздействия на войска и мирное население); завершается эта глава анализом первого десятилетия XXI в., когда информационные и кибероперации обрели свой нынешний облик и были окончательно встроены во внешнеполитический арсенал ряда государств.

Во второй главе рассматривается вопрос о месте информационных и кибероперaций (далее — ИКО) во внешнеполитическом инструментарии современных государств, анализируются произошедшие трансформации этих понятий в отечественной и зарубежной науке. Автор также взял на себя смелость предложить собственные определения ИКО, а также близкого к ним понятия информационной войны для разграничения этих довольно похожих друг на друга явлений.

Третья глава посвящена современным научным подходам к исследованию тематики информационных и кибероперaций, а также смежным темам: дискуссиям о трансформации войны и использованию «мягкой», «анти-мягкой» и «острой» сил; работам по теме манипулирования в интернет-пространстве и социальных сетях, пропаганде и манипулятивным формам убеждения; разбору отдельных кейсов информационных и кибероперaций как инструмента внешней политики.

Появление нового пространства для политики и войны привело к неопределенности в международном праве. Считать ли масштабную «информационную» агрессию нападением на государство? Является ли воздействие на население другого государства посредством СМИ и кампаний в социальных сетях вмешательством во внутренние дела? Общепринятых ответов на эти вопросы пока нет. Но зато уже есть последствия нерегламентированного международным законодательством и правилами проведения информационных и кибероперaций, приведших к дестабилизации политической и социальной обстановки в ряде государств. Только за последнее десятилетие фактически развалилась Ливия, разрушена в огне полугражданской войны Сирия, дестабилизированны Венесуэла и Белоруссия, попала под внешнее управление Украина.

Из-за проведения информационных и кибероперaций, а также из-за мнимых угроз их реализации значительно ухудшились двусторонние отношения ряда государств — например, России

и США. Эрозия десятилетиями создаваемой доверительной атмосферы привела к усилению неопределенности на международной арене и потенциально может привести к глобальному военно-политическому кризису. Одно лишь подозрение в информационном и кибервмешательстве в дела государства может являться причиной сворачивания дипломатических, гуманитарных и военных контактов, послужить поводом для введения санкций, стать причиной ответной кибератаки.

Подобные технологии сегодня доступны не только государствам, но и негосударственным акторам. За примерами далеко ходить не надо — несколько лет назад пропаганда террористических организаций захлестнула социальные сети. Сегодня же глобальные IT-корпорации лишают права голоса политиков и рядовых пользователей, пользуясь возможностью «частной дискриминации».

Угрожающих масштабов достигла киберпреступность. Сегодня несколько человек, вооруженные соответствующими знаниями могут при помощи ноутбуков и выхода в интернет спровоцировать крупный политический скандал или же ограбить банк, находясь буквально за столиком в кафе с бесплатным Wi-Fi. Доказательством этого является фактическое удвоение за последние несколько лет размера ежегодного ущерба от киберпреступности. В 2020 г. он превысил психологическую отметку в 1 триллион долларов, что соответствует 1% мирового ВВП. Отдельные кибератаки против критической инфраструктуры, пока что в теории, могут привести к значительному ущербу, стать причиной гибели людей.

Именно эти вопросы рассматриваются во второй части монографии, включающей гл. 4–7.

В гл. 4 рассматриваются возможности субъектов ИКО как государств, так и негосударственных акторов: террористических группировок, международных IT-корпораций и крупного медиа-бизнеса, различных сообществ в проведении информационных и кибероперациий.

В гл. 5 разбирается роль и место информационных и кибероперациий во внешнеполитическом арсенале некоторых ведущих стран мира: США, Франции, Германии, Великобритании, России и Китая.

Разработанная автором классификация и типология организационных форм, схем, методов и технологий современных информационных и кибернетических операций изложена в гл. 6 данного исследования. В качестве основы было выбрано разделение на три большие группы методов и технологий: подготовки информационного вброса, создания каналов доведения информации,

технического и непрямого действия. Данные методы и технологии используются по отдельности или в комплексе в зависимости от целей и задач информационной или кибероперации.

Глава 7 посвящена проблемам и вызовам, создаваемым проведением ИКО, национальной и международной безопасности. Рассматривается вопрос попытки разработки международного законодательства и рамочных соглашений об ответственном поведении государств в информационном пространстве.

Новые вызовы и возможности не остаются без внимания государств, активно выстраивающих меры противодействия и внедряющих новые инструменты во внутри- и внешнеполитический арсенал. Именно анализу опыта, нормативных наработок и институциональной структуры в области ИКО, проведению информационных операций и действий в киберпространстве ряда ведущих государств мира и некоторых международных организаций посвящена третья часть исследования. К сожалению, объем темы не позволяет рассмотреть опыт всех государств мира в данной области, поэтому выборку пришлось ограничить. Критерием отбора стало наличие опыта в данной области, соответствующих регулирующих документов, масштаб экономик стран (например, Польша обладает довольно развитым инструментарием проведения информационных операций, но в силу ограниченных ресурсов вполне рационально применяет их в одном регионе) и общий военный потенциал.

В гл. 9 рассматривается опыт Соединенных Штатов по организации и проведению информационных и кибернетических операций в сфере внешней политики и деятельности спецслужб. Разбирается ряд руководящих и нормативных документов (начиная от полевых уставов и наставлений ВС США и заканчивая президентскими директивами и внешнеполитическими концепциями).

Глава 10 посвящена опыту Великобритании, Франции, Германии, ЕС и НАТО по проведению информационных операций и кибероборонe.

В гл. 11 разбирается вопрос о построении Китайской Народной Республикой системы информационной безопасности, юридические способы регулирования и цензурирования контента, имеющаяся информация о накопленном КНР опыте проведения информационных и кибероперaций.

Глава 12 посвящена опыту Российской Федерации в области построения ИКО. С учетом того, что на сегодняшний день Россия является мишенью для целого ряда информационных операций зарубежных стран, предпочтение в анализе российской практики в этой области отдано официальным источникам и нейтральным научным публикациям.