

## ВВЕДЕНИЕ

Ситуация на международной политической арене стремительно меняется и вместе с ней меняются технологии борьбы международных акторов. Более того, этот процесс взаимосвязан, поскольку новые средства, методы и формы влияния на противника непрерывно совершенствуются, оттачиваются и апробируются. Значительная часть из них, по сути, является разновидностью неклассической войны, о которой можно прочесть в научной литературе, официальных документах, услышать по телевизору и даже просто от знакомых. Часто эти технологии называют цветными революциями, гибридными войнами, управляемым хаосом, информационными войнами и т.д. Так сложилось, что в силу особой специфики этих явлений термины, которыми их обозначают, в подавляющем большинстве случаев применяют едва ли не по любому поводу. Где есть хотя бы намек на разрушительное, подрывное влияние на какую-либо страну, включая и Россию, но без каких-либо признаков прямой военной агрессии в виде вторжения, сразу же говорят о гибридной войне и т.п. Из-за недостатка понимания и единой, общепризнанной системы описания подобного рода типов неклассической войны возникает чудовищная путаница, вследствие чего отсутствует доминирующий взгляд на указанную проблему, не говоря уже про внятную и проработанную стратегию противодействия новым угрозам. С целью заложить фундамент для единой системы описания (если угодно, системы координат) мы и решили взяться за написание представленной монографии, учитывая опасность отсутствия такой системы. Поясним. Ввиду определенной инерции мышления и некоторой заскорузлости, в экспертной и политической среде, во многих ведомствах, которые в силу своей специфики и возложенных на них функций должны отражать упомянутые угрозы, до сих пор существуют устаревшие представления о таком сложном явлении, как война. Да, за последние годы определенные успехи в осознании специфики новых типов войны были достигнуты, но их все еще критически недостаточно для выработки единой теоретической базы и концепции того, что же представляют собой современные формы и методы насильственного контроля

над целыми государствами, скрытого управления людьми и группами лиц для достижения целей. Или другой пример. До сих пор сохраняется представление о том, что существуют всего три основных типа оружия массового поражения: ядерное, химическое и биологическое. Однако, как будет показано в монографии, которую Вы держите в руках, подобное представление есть опасное заблуждение. Новые виды оружия массового поражения, которыми и являются технологии неклассической войны, по своей разрушительной силе ничуть не слабее, например, ядерной бомбардировки. В то же время с их помощью стало возможным решать те задачи, которые по ряду причин невозможно решить с помощью удара по противнику межконтинентальными баллистическими ракетами с боеголовками мегатонного класса.

Кроме того, книга посвящена новейшим формам и методам информационной войны, проводимой американскими и британскими спецслужбами. Раскрыты механизмы управления чиновниками первого эшелона в США и России на примере конкретных информационных операций. Показано, как с их помощью противники России проходят, как нож сквозь масло, все ее защитные рубежи, доходя до первого лица государства. Наконец, предложены меры противодействия для отражения информационных атак, направленных в том числе и на первых лиц.

Книга разделена на две части. Первая часть посвящена концептуальным основам неклассических войн и таким ее разновидностям, как цветные революции, гибридные и торговые войны.

В первой главе затронуты теоретические вопросы неклассических войн, их происхождение и отличие от войн классических. Для избегания недопонимания и путаницы, даны определения терминам, которые в дальнейшем часто встречаются в книге. Выявлены системные и всеобщие признаки различных типов неклассических войн, благодаря чему был вскрыт их фундаментальный механизм, который лег в основу трех законов неклассической войны. Эти законы являются базой для формирования будущего понятийного аппарата, столь необходимого для единой системы описания, о которой говорилось выше.

Главы со второй по шестую посвящены новейшим разновидностям неклассических войн.

Во второй главе детально рассмотрен так называемый «венесуэльский прецедент» — принципиально новая форма цветной революции, чья схема применима к целому ряду стран, включая и Россию.

В третьей главе рассмотрена гипотетическая эволюционная схема цветного переворота, названная нами *DDoS*-революцией — о том, как сгенерировать протесты сетевых групп в разных регионах большой по площади страны и тем самым исчерпать возможности властей к адекватному и своевременному реагированию на подобные действия.

В четвертой главе показана схема участия американского посольства в несанкционированных протестах в Москве в августе 2019 года.

В пятой главе внимание уделено так называемому миграционному оружию, применявшемуся частью западных элит для инициации распада Евросоюза через достижение нужного результата на референдуме в Великобритании 2016 года, следствием которого стал *Brexit*.

В шестой главе речь идет о противодействии Ирану и Китаю со стороны США. Рассмотрена механика протестов конца 2017 — начала 2018 года в Исламской Республике. Детально изучена схема торговой войны против Китая и ее взаимоувязывание с противодействием китайскому инфраструктурно-логистическому мегапроекту «Один пояс — один путь», а также событиями в Гонконге 2019 года.

Вторая часть посвящена информационным войнам — разновидности неклассических войн, которые могут применяться как совместно с другими типами неклассических войн, так и отдельно от них. Начинается вторая часть с седьмой главы, посвященной понятию «информационная война» и представлению о ней. Детально расписаны уровни ведения информационной войны, что такое информационное оружие и то, какую роль в информационных войнах играют средства массовой информации (СМИ).

Восьмая глава затрагивает вопросы практики организации и проведения информационных операций на примере так называемого «дела об отравлении Скрипалей» — инциденте, произошедшем 4 марта 2018 года в британском городе Солсбери, где был отравлен перебежчик из Главного разведывательного управления (ГРУ) Сергей Скрипаль и его дочь Юлия Скрипаль. «Дело об отравлении Скрипалей» — пример спланированной

и реализованной на высочайшем профессиональном уровне информационной операции против российского руководства. В этой главе она расписана пошагово, с детальным исследованием приемов, использованных организаторами операции. Помимо этого, дан прогноз о том, как данная операция, не исчерпавшая своего потенциала, может быть использована в дальнейшем (ведь мы не знаем, где находятся Скрипали и что с ними стало, да и британские спецслужбы наверняка не выложили все карты на стол).

В девятой главе на примере так называемых «скрипальских чтений» показано, как могла быть осуществлена операция по перехвату информационной повестки дня, если бы в России имелась современная структура, укомплектованная профессионалами, специализирующимися на противодействии информационным войнам.

В десятой главе анализируется такое явление, как фейковые новости, широко используемое в последние годы, представляющее собой инструмент информационной войны. В частности, рассмотрен механизм «вирусного» распространения фейковых новостей и примеры их использования против чиновников самого высокого ранга.

В одиннадцатой главе рассмотрена социальная сеть «Твиттер» как инструмент политического управления и реализации внешней политики США. Наиболее известным из числа политиков-пользователей этой социальной сети является президент США Дональд Трамп. При этом его записи в микроблоге стали не только инструментом политического управления, но могут обернуться и против него.

В двенадцатой главе рассмотрены провокации как метод информационной войны, достигшие на сегодняшний день очень высокого уровня исполнения. На примере двух информационных вбросов, осуществленных американскими газетами *New York Times* и *Wall Street Journal*, показана организация двух провокаций — не достигшей поставленной цели и успешной.

В тринадцатой главе мы затронули технологию контролируемой утечки класса *WikiLeaks*, применявшейся как часть операции по легализации вбрасываемой информации в информационных войнах. В этой технологии ключевым элементом является личность основателя *WikiLeaks* Джулиана Асанджа, чью судьбу (возможно, весьма печальную) при определенных усло-

виях могут использовать для того, чтобы снова задействовать эту платформу с целью легализации очередной порции информации.

В главе четырнадцатой расписан механизм «вклейки» высокопоставленных чиновников в шпионский скандал, связанный с историей Марии Бутиной, которую Федеральное бюро расследований (ФБР) подозревает в работе в качестве иностранного агента без регистрации, да еще сотрудничавшей с российской разведкой. Сам скандал был развернут в форме операции информационный войны, и смысл его состоял в том, чтобы через историю с Бутиной создать возможность компрометации ряда российских и американских чиновников и бизнесменов путем их обвинения в связях с российскими спецслужбами.

В пятнадцатой главе рассмотрены слухи как инструмент информационной войны. Здесь в качестве примера был выбран вброс от имени «военно-дипломатического источника» в одном из уважаемых российских информационных агентств. Согласно ему якобы «американские и британские спецслужбы готовят дезинформацию об окружении президента России В.В. Путина и руководстве Минобороны» по сценарию, напоминающему так называемое «панамского досье» — скандал, вызванный попаданием в открытый доступ секретной информации об офшорных счетах известных политиков, пользовавшихся услугами панамской юридической компании *Mossack Fonseca*. В данной главе мы попытались выявить цели, которые преследовали организаторы вброса.

В шестнадцатой главе речь идет об актуальных проблемах обеспечения информационной безопасности России, а также других стран — участниц БРИКС (Бразилия, Россия, Индия, КНР и ЮАР). Дана оценка перспективным направлениям деятельности России в рамках создания пространства коллективной безопасности БРИКС, а вместе с этим сформулированы задачи формирования пространства информационной безопасности и функции необходимой организационной структуры. Кроме того, предложено создание Российского центра информационных операций БРИКС, предназначенного, прежде всего, для отражения информационных атак, направленных на первых лиц государства. Обозначены как проблемы формирования пространства информационной безопасности БРИКС, так и области сотрудничества и общие потребности стран-участниц в сфере обеспечения ин-

формационной безопасности и противодействия киберугрозам. Расписана дорожная карта для этой цели.

Семнадцатая глава посвящена идее создания «универсального центра противодействия новым вызовам и угрозам», озвученной 15 мая 2019 года секретарем Совета безопасности Российской Федерации Н.П. Патрушевым в Бишкеке на ежегодной встрече секретарей советов безопасности государств — членов Шанхайской организации сотрудничества (ШОС). Решение о создании «универсального центра», как мы полагаем, революционно в свете жизненной необходимости эффективной борьбы с новыми вызовами и угрозами национальной и международной безопасности. В случае успешной реализации данной стратегии не только на базе ШОС, но и БРИКС, Россия будет надежно защищена и прикрыта коллективными усилиями всех стран, входящих в эти объединения.

Наконец, в финальной, восемнадцатой главе говорится о научно-исследовательском испытательном полигоне информационных войн и Центре мониторинга выявления и предупреждения информационных операций. С их помощью планируется подготовка специалистов по противодействию операциям информационных, гибридных и торговых войн.

На этом вводная часть завершена, и мы искренне надеемся, что для Вас, уважаемый читатель, книга будет интересной и познавательной.

### **Благодарности**

Авторы выражают благодарность компании «Промавтоматика» (С. Четвертному и его команде профессионалов высочайшего уровня) в создании инфографики об испытательном полигоне информационных войн и центре мониторинга выявления и предупреждения информационных операций (глава 18); аспирантам МГУ имени М.В. Ломоносова Б.Б. Лавринову и Н.В. Авдеевой, внесших большой вклад в подготовку доклада «Вторжение» (материалы которого сформировали шестнадцатую главу) и в разработку облика концепции кибербезопасности БРИКС; аспирантам МГУ имени М.В. Ломоносова А.В. Курилкину и И.И. Валиуллину, материалы которых легли в основу обзора «Эволюция понятий и представлений об информационной войне», ставшего вступлением к седьмой главе.