ВВЕДЕНИЕ

Настоящая монография посвящена исследованию новейшей практики информационных операций и технологий организации государственных переворотов, особенностей их эволюции, инструментов, модернизации и гибридизации, а также новейших форм и методов противодействия им. Ее главная задача — зафиксировать технику, способы, формы и методы современных информационных операций, проведенных Россией и США «после Крыма», и сделать их доступными для широкой читательской аудитории — до того, как особо ответственные граждане не навесят на все это гриф «совершенно секретно».

Современные информационные войны и цветные революции переживают период стремительной гибридизации: они становятся комплексными, вбирают в себя опыт и «лучшие практики» других видов борьбы, тем самым приспосабливаясь к различным форматам и условиям ведения боевых действий. Особенно хорошо это заметно на примере современных цветных революций. Появление в 2019 г. в Венесуэле новой технологии организации государственных переворотов (так называемого Венесуэльского прецедента), сочетающей в себе массовые протесты (по майданному сценарию) «снизу» с активной психологической «обработкой» окружения лидера страны «сверху», на годы вперед определило направление эволюции всех «цветных» технологий. По тому же майданному сценарию происходили массовые протесты в Белоруссии в 2020 г. В ходе «цветной революции» в Гонконге (в 2019–2020 гг.) к технологии, разработанной первоначально только для Венесуэлы, добавились технологии связи и координации протестных групп, конфликтной мобилизации под неполитическую повестку, впервые апробированные в ходе «электромайдана» 2015 г. в Армении, а также технологии организации протестующих масс в «рой» (наподобие пчелиного, обладающего бóльшей мобильностью, чем просто агрессивная толпа), некоторые элементы которых, возможно, впервые были опробованы при организации протестов в Москве (до и после выборов в Мосгордуму 2019 г.) и в Хабаровске (2020 г.). В этих же условиях информационные операции окончательно перестают

быть только «агрессивными информационными кампаниями» и становятся оперативными комбинациями, в которых на передний план выдвигается оперативно-агентурная и оперативно-розыскная работа, сочетаемая с использованием новых методов управления сознанием и поведением граждан.

Появление новых гибридных по своей природе форм и методов неконвенционной борьбы потребовало выработки новых подходов к противодействию данным угрозам — таких же комплексных и гибридных, как и противостоящие им методы и технологии нападения.

В монографии подробно раскрываются основные формы, схемы, элементы информационных операций современного типа, ведущих свое начало от «Панамского досье» 2016 г.; на примере публикаций в New York Times (24.05.2019) и Wall Street Journal (03.06.2019) демонстрируется, какими бывают информационные вбросы и для чего они предназначены. На примере конкретных информационных операций («Пражский инцидент» с рицином 2020 г., заявление С. Райс «Российская методичка по организации госпереворотов» 2020 г., «Дело об отравлении Скрипалей» 2018–2020 гг., «Венесуэльский прецедент» и «операция Гедеон» 2019–2020 гг.) раскрывается, каким образом информационные вбросы используются в современных тактических (оперативных играх) и стратегических операциях информационной войны. Кроме того, выделяются генеральные линии и основные стратегии ведения информационной войны против России. На примере российской практики проведения информационных контроопераций («Дело Кабельо» 2019 г., «Скрипальские чтения» 2019 г., «Поиск русского крота в ЦРУ» 2019 г. (оперативная игра с Р. О'Брайеном) и др.) раскрываются новейшие формы и методы организации противодействия информационным операциям иностранных государств и оперативным играм иностранных разведок.

Благодарности

Мы выражаем искреннюю благодарность выдающемуся психологу профессору Анатолию Ивановичу Петренко, внесшему ценнейший вклад в разработку «Плана первоочередных мероприятий…» (разд. 7.4), выдержки из которого использовал президент РФ; ветерану боевых действий в Демократической республике Афганистан, заместителю руководителя РСВА Владиславу Ивановичу Теличко за его решающий вклад в разработку и реализацию новейшей методики организации противодействия

фейковым новостям (разд. 5.4); выдающемуся аналитику Константину Сергеевичу Стригунову, одному из авторов и организаторов провала ЦРУ в августе 2019 г. («Дело Кабельо», разд. 4.2), настоящему разведчику, директору частной разведывательной компании «Р-Техно» Роману Владимировичу Ромачеву, первому вскрывшему связь республиканского сенатора Митча Макконелла (Mitch McConnell) с российским антифейковым проектом «Вбросам.нет», а также Сергею Четвертному, исполнительному директору компании «Промавтоматика», и его команде, внесшим вклад в разработку идеологии и первоначальной архитектуры технических средств поддержки (разд. 7.3).

ГЛАВА

1

Технологическая революция в сфере информационных войн: информационные операции нового типа

Настоящая глава посвящена систематизации и классификации новейшей практики информационных операций — ключевых элементов информационной войны. Информационные войны в современном мире стали привычным фактором окружающей действительности. Современная информационная война — это особый вид вооруженного конфликта, в котором столкновение сторон происходит в форме информационных операций с применением информационного оружия. Ее главная задача — разделить и поляризовать общество, разорвать его на множество фрагментов, искренне ненавидящих друг друга, с тем, чтобы затем столкнуть их между собой, инициировав борьбу на уничтожение, или объединить их агрессию в единый поток и направить его против действующей власти. При этом цель информационной войны — сломить волю противника к сопротивлению и подчинить его сознание. Высокая эффективность информационных операций и растерянность, являющаяся типичной реакцией большинства стран, делают информационные войны одним из основных элементов современных гибридных вооруженных конфликтов [4].

Однако так было не всегда. Всего лишь каких-то 5–7 лет назад к применению методов информационного, психологического и кибернетического воздействия относились с опаской: они были несовершенны, не давали гарантированного результата, несли высокие риски раскрытия установочных данных на самих

организаторов нападения и использовались в основном в сочетании с более надежными, мощными и отлаженными методами прямой военной агрессии.

Информационные операции и атаки, столь распространенные сегодня, еще совсем недавно присутствовали практически исключительно в деятельности спецслужб и были элементами оперативных игр, разыгрываемых разведками в стиле шахматных партий или сеансов игры в покер. Ситуативность разработки сценария самих оперативных игр и преследуемые ими сугубо тактические цели, вызванные желанием чем-нибудь «зацепить» противника или на чем-нибудь его подловить, не давали возможности выйти информационным операциям на оперативный простор. В этом контексте сам термин «информационная война» на протяжении многих десятилетий не воспринимался серьезно: его считали ловкой находкой журналистов, пытающихся таким образом увеличить тираж своих изданий. Похоже, серьезно к информационным операциям с самого начала относились только военные США, которые уже в 1988 г. внедрили термин «психологическая операция» в полевой устав Армии США (FM 33.1-1).

Сами же информационные операции в тот период (предшествующий их технологической «революции» в 2014 г.) начали формироваться как самостоятельный вид деятельности, но в их планировании продолжает преобладать ремесленный подход: каждая операция разрабатывается индивидуально, как уникальный образец, под нее подбирается такая же уникальная (и неповторимая, заточенная под конкретные особенности конкретной оперативной остановки) схема организации, не похожая ни на одну из предыдущих. Это шедевр, произведение оперативного искусства, не гарантирующий конечного результата. В этом плане методы прямой военной силы выглядели как более надежные и, если ситуация позволяла, как более предпочтительные.

Однако, в 2014 г. все в одночасье изменилось: Крым, с ужасом взиравший на осуществленный в Киеве государственный переворот, сделал «ход конем» и добровольно вошел в состав Российской Федерации. Для Запада и некоторой части Востока это решение стало настоящим шоком: похоже, ни США, скупавшие в Крыму детские садики и школы для обеспечения комфортного размещения детей американских военнослужащих, планировавшие покрыть Крым сетью военных баз, ни Турция, рассчитывавшая на такие же условия для своих военных и планировавшая

в обозримом будущем (на волне распада украинской территории) вообще забрать Крым себе, такого от крымчан не ожидали. Возможность прямого военного вмешательства в форме, например, высадки десанта, имелась, но была упущена вследствие растерянности американских генералов, граничащей с паникой: когда же они пришли в себя и вернули себе способность адекватно оценивать происходящее, Крым уже был российским, а время — безнадежно упущено. В этом плане у США остался только один инструмент агрессивного ответа — информационные операции.

Ситуация с внезапным «побегом» Крыма из Украины и вхождением в состав Российской Федерации побудила специальные службы США реагировать немедленно, на ходу, «с колес», без раздумий, поскольку «времени на раскачку», как верно заметил президент РФ В.В. Путин[1], у них уже не было. В этом плане прежние подходы к ведению информационных войн, отличающиеся высокой избирательностью, не годились: в 2014 г. США остро нуждались именно в массовом проведении информационных операций, следовавших одна за другой так, как будто все их произвели на одном и том же конвейере (как автомобили на заводах Г. Форда). Это, в свою очередь, привело США к переводу процессов планирования, организации и проведения информационных операций на промышленные рельсы, став своего рода «промышленной революцией» в сфере информационных войн. Промышленный же подход, в свою очередь, привел к унификации и стандартизации организационно-технологических схем информационных операций, которые в итоге дали одну единственную универсальную базовую схему, появившуюся у американских спецслужб предположительно к лету 2015 г. Эта схема впервые получила свое «боевое крещение» в печально знаменитом скандале с «Панамским досье» (2016 г.): в этом деле стандартная англо-саксонская схема информационных операций, представляющая собой итерационную последовательность вбросов и технологических пауз («периодов тишины»), присутствует в чистом, незамутненном и абсолютно незамаскированном виде; ее легко можно разглядеть даже неспециалисту, даже невооруженным взглядом. Благодаря этой схеме «Панамский скандал», как известно, имел грандиозный успех; с этого самого момента все информационные операции спецслужб США становятся репликой с «Панамского досье» — исполняются по одному и тому же, многократно повторяющемуся, шаблону.

[1] «Времени на раскачку нет» — одна из самых знаменитых цитат В.В. Путина.

Новые технологические решения, выработанные США в сфере ведения информационных войн, не только дали возможность повысить частоту проведения самих операций (т.е. поставить их производство на конвейер), но и позволили испытывать на этой платформе различные оперативные сценарии и сюжеты, сделавшие современные информационные операции похожими на телевизионные детективы или «мыльные оперы». Так, в «Деле об отравлении Скрипалей» (совместной операции британских и американских спецслужб, продолжающейся и в настоящее время) только в течение 2018 г. были отработаны два сценария — «игра с пошаговым повышением ставок» и «ловля на живца» (на заранее вывешенную приманку); в скандале с так называемым аргентинским кокаином — «ловля на приманку», в роли которой выступал сам кокаин, арестованный аргентинской полицией безопасности; «Дело Марии Бутиной» — «ловля на живца», причем в роли «живца» выступила сама фигурантка дела, задержанная ФБР за создание в США «российской шпионской сети»; история с перехватом в Генте в 2018 г. крупной партии кокаина, промаркированной символикой, похожей на символику «Единой России», — «наклеивание ярлыков»; «выборы в Интерпол» (ноябрь 2018 г.), завершившиеся срывом избрания российского кандидата А. Прокопчука, — сценарий «скрытой угрозы» (как в «Звездных войнах»); и т.д. Благодаря этим сценариям информационные операции превратились в тонкую многоходовую психологическую игру.

1.1. Гибридизация современных вооруженных конфликтов

В свою очередь, технологическая «революция» в сфере информационных войн, произошедшая в 2014–2015 гг., фактически подтолкнула процесс объединения (или, если точнее, «сборки») различных невоенных форм силового подавления противника под общим «зонтичным» брендом. Таким «зонтичным брендом» стал термин «гибридные войны», придуманный Ф. Хоффманом в еще 2007 г. [20], но все это время мирно прозябавший где-то на периферии дискуссий о природе современной войны. Нынче его «вытащили из нафталина» и придали ему новое доктринальное звучание: теперь это уже не экзотика, а полноценная военная стратегия, предусматривающая одновременное комбинированное использование различных видов

неконвенционной вооруженной борьбы — информационных, дипломатических, экономических («торговых») войн, диверсионно-подрывных операций (таких как современные цветные революции), нередко сопровождающихся применением методов, характерных для транснациональных преступных организаций, сетевых террористических группировок III (таких как Аль-Каида[2]) и IV (таких как ИГИЛ[3]) поколения, наркокартелей и т.д. В этих войнах традиционные боевые операции вооруженных сил не потеряли своей значимости [2], но стали использоваться реже (по сравнению с теми же «торговыми войнами»), избирательнее и в основном для публичного «наказания» и унижения и так уже сломленного противника, утратившего волю к сопротивлению. Такого противника сначала «ломают» с помощью информационной, торговой, дипломатической войны, партизанских (повстанческих), диверсионно-террористических операций (включая акции так называемого «государственного терроризма»[3]), а затем публично «добивают» с помощью прямого вооруженного вторжения (интервенции).

Возникновение и стремительное развитие новых форм и методов вооруженной борьбы невоенного характера (гибридных, информационных, торговых войн, новых форм повстанческих войн и т.д.) привело к существенному изменению качественного состава ее участников. Вместо регулярных армий на передний план выдвинулись:

- криминальные, мафиозные вооруженные формирования транснациональных структур организованной преступности, среди которых особое место заняли наркокартели;
- вооруженные формирования международных террористических организаций и группировок;
- незаконные вооруженные группировки экстремистского характера, существующие «под крышей» (под патронажем) специальных служб различных государств (так называемые «прокси»-формирования, или «зелень»);
- «титушки», иррегулярные полукриминальные группировки, негласно поддерживаемые и подпитываемые официальными властями (с помощью которых подавляются протесты в стране, т.е. опосредованно применяются методы террора в отношении несогласного населения; такие как

[2] Аль-Каида и ИГИЛ — террористические организации, запрещенные в РФ.

[3] Государственный терроризм (юр.) — форма применения насилия, когда одно государство использует методы террора против другого государства. Объектом государственного терроризма может быть только государство в целом.

«коллективос» в Венесуэле, «титушки» на Украине, «прокси» в Сирии и Ливии и др.);
- наемники;
- родовые, племенные ополчения, возглавляемые племенными вождями (шейхами), характерные для регионов, где сохранились родоплеменной уклад и трайбалистское устройство общества.

Именно эти неклассические акторы идеально подходят для ведения гибридных войн нового типа — особой мобильной диверсионно-террористической квази-повстанческой войны, на три четверти состоящей из тайных операций и оперативных комбинаций спецслужб (включая разведки наркокартелей, транснациональных ОПГ и т.д.), в которых традиционные армии оказываются слишком неповоротливыми и поэтому бессильными. При этом в плане качества и структурной сложности новых акторов наблюдаются регресс и возвращение к архаике: снова в региональных вооруженных конфликтах значительную роль начинают играть разнообразные родоплеменные ополчения, возглавляемые племенными вождями и военачальниками, набранными из местной знати, организованные по криминальному принципу банды наркокартелей и сцементированные примитивной средневековой идеологией (создававшейся для неграмотных бедуинов) террористические организации типа ИГИЛ[4].

Переходное место в этой линейке неклассических акторов заняли частные военные кампании (ЧВК), ставшие чем-то средним между наемничеством, криминалом и регулярными армейскими формированиями. Стремление некоторых ЧВК сохранить армейскую или полицейскую структуру (т.е. выстроить свою деятельность по регулярному — армейскому — принципу) дало им возможность легализоваться и использовать (частично) в проводимых ими боевых или обеспечивающих операциях преимущества регулярных форм ведения боевых действий. Однако, став регулярными ЧВК, эти структуры потеряли мобильность, присущую вооруженным отрядам наркокартелей и террористических группировок.

С приходом в сферу ведения современных войн новых видов неклассических акторов изменился и сам характер ведения боевых действий: войны стали сетевыми, или сетецентричными, что характерно для разведывательно-диверсионной, карательной,

[4] Террористическая организация, запрещенная в РФ.

террористической, повстанческой/партизанской и контрпартизанской деятельности. При этом многие военные эксперты называют это явление «войнами шестого поколения» (теми самыми, о приходе которых В. Слипченко писал еще в 2002 г. [14]) и связывают его с развитием военного искусства, появлением новых форм и методов ведения вооруженной борьбы, особенно эффективных в условиях «глобальной неопределенности» и общей разбалансировки системы международных отношений [16]. Соглашаясь в целом с тем, что развитие военного искусства может привести к переходу войн в сетевую плоскость, с неизбежной архаизацией, отметим, что сетевая форма современных гибридных войн связана, скорее, не с особыми преимуществами ее стратегии и тактики, а с принципиальной неспособностью выстроить эффективную и универсальную систему оперативного управления всеми видами неклассических акторов, участвующих в ней: с боевыми формированиями наркокартелей или иных транснациональных преступных группировок приходится взаимодействовать одним образом, с племенными ополчениями — другим, с «титушками» — третьим, и т.д. В итоге выходит, что все эти силы и средства одновременно могут быть задействованы только в войне, построенной по сетевом принципу.

Однако такая пестрота и неунифицируемость (принципиальная несводимость к единому знаменателю) акторов несет в себе и определенные преимущества, позволяющие вести войну по «проектному» принципу. Так, если необходимо провести конкретную боевую операцию в определенном регионе, где действуют наркокартели или повстанцы, ресурс для этой операции можно собрать прямо на месте из «деталей конструктора»: военную силу позаимствовать у радикальных повстанческих движений или ЧВК (можно задействовать армейский или полицейский спецназ), систему снабжения и связи предоставят в распоряжение наркокартели, диверсантов дадут «прокси» или террористические группировки, разведку обеспечат трансграничные структуры организованной преступности, деньги на операцию предоставит торговля кокаином или синтетическими наркотиками, которые всегда можно обменять на оружие или боевиков, а «народ» и «демократию» будут представлять шейхи — племенные вожди. При этом все компоненты в наличии и уже присутствуют в регионе в «разобранном состоянии»; их остается только собрать в определенной конфигурации и под конкретную задачу.

1.2. Гибридизация технологий организации государственных переворотов (цветных революций)

Гибридизация, выведшая информационные войны на новую ступень эволюции, затронула и другие виды неклассических войн, вынуждая и их активно приспосабливаться к веяниям времени. При этом в информационных операциях появился новый инструмент воздействия — фейки, сочетание которых с вирусными технологиями распространения (использующими механизм «эмоционального заражения» для быстрой передачи фейка от одного человека к другому) сделало их «абсолютным оружием», от которого нет спасения[5].

В сфере организации государственных переворотов, где первую скрипку на протяжении почти 20 лет играли технологии цветных революций, напротив, внезапно наметился откат к прежним схемам «дворцовых» переворотов и мятежей, в которых главу государства отстраняют от власти, договорившись с людьми из его ближайшего окружения, а массовые протесты и беспорядки, организованные по канонам цветных революций, разворачиваются исключительно для отвлечения внимания действующей власти (на «негодный объект»).

Видимо, мода на цветные революции прошла, определив «закат» идей Дж. Шарпа: в Боливии и Венесуэле в 2019 г. эти технологии уже не имели самостоятельного значения. В определенном смысле исключением из этого правила стала «Белорусская весна» 2020 г. (попытка осуществления цветной революции в Беларуси), в которой внешне хорошо различимые и идентифицируемые «цветные» технологии госпереворота тоже подверглись гибридизации, став «точкой сборки» для «лучших практик» организации цветных революций на постсоветском пространстве. Общая схема организации цветной революции в Беларуси точно копирует киевский майдан 2013–2014 гг. (но без самого майдана — постоянно действующего лагеря), технологии связи и координации протестных групп взяты из Гонконга 2019–2020 гг., технологии конфликтной мобилизации под неполитическую повестку заимствованы у ереванского «электромайдана» 2015 г. Общая схема государственного переворота при этом является точной копией «Венесуэльского прецедента» — технологии

[5] Спайка фейков и вирусных технологий произошла в 2016 г. в период президентской избирательной кампании в США. См.: [10].