ВВЕДЕНИЕ

Настоящее учебное пособие посвящено систематизации и классификации новейшей практики информационных операций (ИО) — ключевых элементов информационной войны (ИВ). Ее главная задача — зафиксировать технику, способы, формы и методы современных ИО, проведенных Россией и США «после Крыма», и сделать их доступными для широкой читательской аудитории.

Современные ИВ 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 организацию массовых протестов (по майданному сценарию) «снизу» с активной психологической «обработкой» окружения лидера страны «сверху», на годы вперед определило направление эволюции всех «цветных» технологий; в массовых протестах в Белоруссии 2020 г., также построенных по «майданному» сценарию. К этим технологиям (выработанным первоначально только для Венесуэлы) добавились технологии связи и координации протестных групп, выработанные в ходе «цветной» революции в Гонконге (2019–2020), технологии 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 боль-

шей 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 ИО 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 этих 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 ИО современного типа, ведущие 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 ИО («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, как именно информационные вбросы используются в современных тактических (оперативных играх) и стратегических операциях ИВ; выделяются генеральные линии и основные стратегии ведения ИВ против России. На примере российской практики проведения информационных контроперациий («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 ИО иностранных государств и оперативным играм иностранных разведок.

Технологическая революция в сфере информационных войн: информационные операции нового типа

ИВ в современном мире стали одним из привычных факторов окружающей нас действительности. Современная ИВ — это особый вид вооруженного конфликта, в котором столкновение сторон происходит в форме ИО с применением информационного оружия. Главная задача ИВ — разделить и поляризовать общество, разорвать его на множество клочков и фрагментов, заставить эти фрагменты искренне ненавидеть 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 ИВ — сломить волю противника к сопротивлению и подчинить его сознание своей воле. Высокая эффективность ИО и растерянность, являющаяся типичной реакцией большинства стран на акции информационной войны, делают ИВ одним из основных элементов современных гибридных вооруженных конфликтов[1].

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 в себе 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.

ИО и атаки, столь распространенные сегодня, еще 5–6 лет назад присутствовали практически исключительно в деятельности спецслужб и были элементами оперативных игр, разыгрываемых разведками в стиле шахматных партий или сеансов игры в покер; ситуативность складывания сценария самих оперативных игр и преследуемые ими сугубо тактические цели, вызванные желанием чем-нибудь «зацепить»

[1] См.: *Манойло А.В.* Информационная война и новая политическая реальность: Ч. I // Вестник Московского государственного областного университета. 2021. № 1. URL: www.evestnik-mgou.ru

противника или на чем-нибудь его подловить, не давали возможности выйти ИО на оперативный простор. В этом контексте сам термин «информационная война» на протяжении многих десятилетий не воспринимался серьезно: его считали ловкой находкой «газетчиков», пытающихся таким путем поднять тираж своих изданий. Похоже, серьезно к ИО с самого начала относились только военные США, уже в 1988 г. внесшие термин «психологическая операция» в полевой устав Армии США (FM 33.1-1).

Сами же ИО в тот период (предшествующий их технологической «революции» в 2014 г.) уже начинают складываться 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 народа Крыма 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 взять 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 — ИО.

Ситуация с внезапным «побегом» Крыма из Украины и вхождением в состав Российской Федерации побудила специальные службы США реагировать немедленно, на ходу, «с колес», без времени на раздумья, поскольку времени на раскачку, как верно заметил наш президент В.В. Путин[2], у них уже не было. В этом плане прежние подходы к ведению ИВ, отличающиеся высокой избирательностью, не годились: в 2014 г. США остро нуждались именно в массовом проведении ИО, 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 в США к переводу процессов планирования, организации и проведения ИОна промышленные рельсы, став в сфере ИВ своего рода «промышленной революцией». Промышленный же подход, в свою очередь, привел к унификации и стандартизации организационно-технологических схем ИО, 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 ИО, 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 ИО спецслужб США становятся репликой с «Панамского досье» — исполняются по одному и тому же, многократно повторяющемуся, шаблону.

Новые технологические решения, выработанные США в сфере ведения ИВ, не только дали возможность повысить частоту проведения самих операций (т.е. поставить их производство на конвейер), но и позволили испытывать на этой

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

платформе различные оперативные сценарии и сюжеты, сделавшие современные ИО 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 одного 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» (ЕР), — «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 ИО превратились в тонкую многоходовую психологическую игру.

Гибридизация современных вооруженных конфликтов

В свою очередь, технологическая «революция» в сфере В, 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 еще в 2007 г.[3], но все это время мирно прозябавший где-то на периферии дискуссий о природе современной войны. Теперь же его «вытащили из нафталина» и придали ему новое доктринальное звучание: это уже не экзотика, это — полноценная военная стратегия, предусматривающая одновременное

[3] *Hoffman F.G.* Conflict in the 21st century: The rise of hybrid wars [Электронный ресурс]. [2007]. URL: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf (дата обращения: 29.12.2020).

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») и IV (таких как ИГИЛ[4]) поколений, наркокартелей и т.д. В этих войнах традиционные боевые операции вооруженных сил не потеряли своей значимости[5], 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»[6]), 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 повстанческой войны и т.д.) привели к существенному изменению качественного состава ее участников; взамен 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)

---

4 «Аль-Каида» и ИГИЛ – террористические организации, запрещённые в РФ.

5 *Калдор М.* Новые и старые войны: организованное насилие в глобальную эпоху / пер. с англ. М.: Изд-во Института Гайдара, 2016. 416 с.

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

специальных служб различных государств (так называемые «прокси»-формирования, или «зелень»);
- «титушки», иррегулярные полукриминальные группировки, негласно поддерживаемые и подпитываемые официальными властями (с помощью которых власти давят протесты в стране, т.е. опосредованно применяют методы террора в отношении несогласного населения; такие как «коллективос» в Венесуэле, «титушки» на Украине, «прокси» в Сирии и Ливии и др.);
- наемники;
- родовые, племенные ополчения, возглавляемые племенными вождями (шейхами), характерные для регионов, на которых сохранились родоплеменной уклад и трайбалистское устройство общества.

Именно эти неклассические акторы идеально подходят для ведения гибридных войн нового типа — особой мобильной диверсионно-террористической квазиповстанческой войны, на три четверти состоящей из тайных операций и оперативных комбинаций спецслужб (включая разведки наркокартелей, транснациональных организованных преступных группировок (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 племенной знати, организованные по криминальному принципу банды наркокартелей и сцементированные примитивной средневековой идеологией (создававшейся для неграмотных бедуинов) террористические организации типа ИГИЛ[7].

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 — армей-

[7] Организация запрещена в РФ.

скому — 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, террористической, повстанческой / партизанской и контрпартизанской деятельности. При этом многие военные эксперты стали называть этот вид войн войнами шестого поколения (теми самыми, о приходе которых В. Слипченко писал еще в 2002 г.[8]) и связывать с развитием военного искусства, появлением новых форм и методов ведения вооруженной борьбы, особенно эффективных в условиях «глобальной неопределенности» и общей разбалансировки системы международных отношений[9]. Соглашаясь в целом с тем, что развитие военного искусства может привести к переходу войн в сетевую плоскость с неизбежной архаизацией, все же 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 гибридной войне на твоей стороне: в этой войне 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.

---

[8] *Слипченко В.* Войны шестого поколения. Оружие и военное искусство будущего. М.: Вече, 2002. 384 с.

[9] *Хаас Р.* Мировой беспорядок. Американская внешняя политика и кризис старого порядка / пер. с англ. М.: АСТ, 2019. 320 с.

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 можно взять у радикальных повстанческих движений или ЧВК (можно взять и 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 даст кокаин или синтетические наркотики, которые всегда можно обменять на оружие или боевиков, а «народ» и «демократию» будут представлять шейхи — племенные вожди. При этом все компоненты уже в наличии и присутствуют в регионе в «разобранном состоянии»; их остается только собрать в определенной конфигурации и под конкретную задачу.

Гибридизация технологий организации государственных переворотов («цветных» революций)

Гибридизация, выведшая ИВ на новую ступень эволюции, затронула и другие виды неклассических войн, вынуждая и их тоже активно гибридизироваться, приспосабливаясь тем самым к веяниям времени. При этом в ИО 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[10]; а в сфере организации государственных переворотов, в которой первую скрипку

[10] Спайка фейков и вирусных технологий произошла в 2016 г. в период президентской избирательной кампании в США. См.: *Манойло А.В.* Фейковые новости как угроза национальной безопасности и инструмент информационного управления // Вестник Московского университета. Серия 12 «Политические науки». 2019. № 2. С. 41–42.

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 Белоруссии), 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: так, общая схема организации «цветной» революции в Белоруссии 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 организации госпереворота в Венесуэле в 2019 г. Собственно белорусского в минских протестах немного: своя аутентичная символика, фактическое отсутствие майдана (который можно было бы блокировать, накрыть и разогнать) — он теперь подвижен, как цыганский табор, и перемещается с толпами протестующих; и… широкое использование нового средства протестной коммуникации — *Telegram*-каналов.

Но и это исключение только подтверждает правило: схема государственного переворота в Белоруссии как две капли воды повторяет (а точнее, копирует) технологию

«венесуэльского прецедента». В этом плане попытка переворота в Белоруссии — не совсем «цветная» революция, точнее, совсем не «цветная»; это «верхушечный» («дворцовый») госпереворот, в котором лидера страны должны сместить свои же ближайшие друзья и соратники, предварительно обговорив все детали с организаторами смены режима — с США, а «цветная» революция в Белоруссии — только для отвода глаз (для отвлечения внимания А.Г. Лукашенко и Москвы на «негодный объект»). Этой технологии, едва не опрокинувшей режим Н. Мадуро в 2019 г., А.Г. Лукашенко пытался противопоставить метания, «стендап» и практику импровизаций.

Благодарности. Мы выражаем искреннюю благодарность 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 (п. 5.4); выдающемуся аналитику Константину Сергеевичу Стригунову, одному из авторов и организаторов провала ЦРУ в августе 2019 г. («Дело Кабельо», п. 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»; моим ученикам А.В. Курилкину и И.И. Валиуллину, материалы которых легли в основу раздела 1.1 главы 1; моей ученице А.Э. Попадюк, совместно с которой написан раздел 1.2 главы 1; а также Сергею Четвертному, исполнительному директору компании «Промавтоматика», и его команде, внесшим вклад в разработку идеологии и первоначальной архитектуры технических средств поддержки (п. 8.3).

Этические нормы и принципы. Настоящее учебное пособие не содержит материалов, критикующих деятельность органов исполнительной власти Российской Федерации. Мы с ува-

жением относимся к деятельности Администрации Президента, МИД, иных министерств и ведомств Российской Федерации, в нынешних предельно непростых условиях несущих колоссальную нагрузку по управлению страной и ответственность за ее настоящее и будущее. С таким же неизменным уважением мы относимся к их лидерам. Вместе с тем, разбирая примеры операций, в которых Российской Федерации не удалось перехватить у своих противников оперативную инициативу, мы стремились не лакировать действительность, поскольку ошибки ценны именно тем, что умные люди на них учатся.

При планировании, организации и проведении специальных операций нельзя недооценивать противника, даже если ты лично к нему очень плохо относишься. Практика показывает, что даже такой серьезный и подготовленный противник, как разведывательные службы США, при определенном стечении обстоятельств действительно может вести себя весьма неумело, совершать почти детские ошибки и поддаваться панике. Если такое происходит (как это было в «деле Кабельо» в Венесуэле в 2019 г.), тем лучше для нас, так как в этом случае любой просчет противника может обернуться нашей победой. Однако рассчитывать на такое везенье априори не стоит. Лучше переоценить противника, чем его недооценить и потом заплатить за это непомерно высокую цену.

Предупреждение. Все встречающиеся в тексте настоящего учебного пособия названия международных террористических организаций, таких как «Исламское государство» («Исламское государство Сирии, Ирака и Леванта», ИГИЛ, ИГ, ДАИШ), «Аль-Каида», «Братья-мусульмане», «Талибан», «Джебхат ан-Нусра» («Хайят Тахрир аш-Шам», ХТШ), «Джейш аль Ислам», «Ахрар аш-Шам», «Исламский фронт», «Хизб ут-Тахрир» и др., принадлежат международным террористическим организациям, запрещенным в Российской Федерации, и используются исключительно в научных и учебных целях.