ВВЕДЕНИЕ

Учебное пособие, которое Вы, уважаемый читатель, держите сейчас в руках, посвящено информационным войнам и психологическим операциям, из которых эти самые войны состоят. Кроме того, в этой книге, помимо сведений об информационных войнах, Вы обязательно найдете еще множество сведений, которые должен знать специалист в области информационных и гибридных конфликтов.

Самой главной частью этой книги, безусловно, является вторая глава, где детально описаны новейшие организационные схемы операций информационной войны и разобраны механизмы их действия, демонстрирующие, как подбирают, изучают и обрабатывают будущую жертву информационной атаки, как «выносят ей мозг», предварительно подведя эмоции к наивысшей для данного конкретного человека точке кипения, в которой он полностью утрачивает над собой контроль и начинает метаться, как бешеный скунс, оказавшийся в клетке. Как находят подход практически к любому человеку, вычислив его доверительные контакты и каналы коммуникации. Как организуют контролируемые утечки компромата, получившие название операций легализации вбрасываемой информации. И как со всем этим жить.

Вместе с тем информационные войны и психологические операции ведутся не в вакууме — они разворачиваются в социальной среде, в том самом обществе, живя в котором, по словам классика, нельзя быть от него свободным. Эту социальную среду, питающую информационные войны и обеспечивающую психологическим операциям и атакам заданную эффективность в поражении живых целей (мишеней информационной агрессии), формируют политические конфликты, малые и большие войны, рейдерские захваты, беспощадная борьба ведущих стран мира друг с другом и иногда всех вместе — с международным терроризмом. Все эти процессы непрерывно осложняются (если не сказать — отягощаются) идущими процессами гибридизации (войн, мировой политики, всего на свете), на которые к тому

же сверху накладывается идущее вкривь и вкось формирование новой многополярности. Если ко всему этому добавить еще и типично хулиганские порывы США вмешиваться в выборы всех без исключения президентов во всех странах мира, включая свою собственную (а потом все сваливать на других), то получится такой винегрет, в котором и без информационных войн достаточно сложно выжить. Но именно поэтому знать этот мир необходимо — хотя бы навскидку, штрихами. Иначе не удастся правильно выбрать тот момент, единственный и неповторимый, когда именно применение тщательно продуманной и очень хорошо спланированной информационной операции способно мгновенно выбить противника из седла, да так, что он больше в это седло никогда уже не сядет.

Путь к истине иногда бывает тернист и запутан. Именно поэтому данная книга начинается не с обсуждения информационных войн (т.е. с извечных вопросов, волнующих человечество на протяжении многих веков: «Что сие гой еси?», и «Откель есть пошла войня информячая?», и «Почему у нее все не как у людей?»), и даже не с разговора о психологических операциях, а с главы, посвященной гибридизации мировой политики и анатомии международных конфликтов, т.е. с политпросвета. Хотя конфликты в этой главе расписаны четко, академично и системно, как в учебнике: с разбором всех их типов и структур, таким образом, что больше их ни с чем уже не спутаешь. Ни с бульдогом, ни с носорогом. Оно в принципе и понятно: информационная война сама является международным, вооруженным, исключительно хитро сделанным конфликтом, и гасить его приходится примерно теми же методами, которыми в обычной международной практике достигаются его урегулирование или разрешение.

Во второй главе вы найдете детальное описание современных технологий информационных войн, применяемых в международных отношениях и мировой политике: схемы, методы, технологии. Цель этой главы — не только сформировать представление о новейших формах и методах политической борьбы в информационной сфере, особенностях планирования и осуществления информационных атак на первых лиц государства, но и научиться с ними бороться. Поможет этому осознание того

факта, что у американцев в плане проведения информационных операций нет видового разнообразия: большинство наиболее опасных из них (таких как известный скандал с панамскими офшорами или скандально известное «Дело Скрипалей», «Аргентинский кокаиновый скандал», «Кремлевский доклад» Минфина США) имеют в основе одну и ту же единственную стандартную организационную схему, представляющую собой последовательность информационных вбросов, разделенных периодами экспозиции (информационной «тишины») и согласованных по времени, целям, задачам и объектам воздействия. В этом плане специалист легко их просчитает и в нужный момент пнет ногой в уязвимое место американскому агрессору, страх потерявшему. Ведь на самом деле противодействие информационным операциям противника — это оперативные комбинации, сочетающие организационные и информационные (информационно-психологические) методы воздействия, им можно и нужно противостоять. В результате у читателей появляется возможность приобрести практические навыки противодействия информационным атакам, вбросам и иным методам информационного давления, применяемым в современной политической борьбе. А также узнать, почему Джен Псаки и Мэтью Ли — не муж и жена, а четыре совершенно разных человека, почему Мария Захарова так и не стала «нашим ответом на Псаки», и какую роль все эти персонажи играют в разведывательных операциях контролируемой утечки, известных в теории информационных войн как «операции по легализации вбрасываемой информации».

У читателя есть возможность самому убедиться, что все приемы и методы информационной войны предельно просты, имеют в основе простые схемы и решения, основаны на безусловном срабатывании в нужный момент элементарных психологических реакций и на своевременном считывании столь же простых рефлексивных реакций мишени атаки, эмоционально реагирующей на направленное на нее адресное информационное воздействие. Но в этом и состоит гениальность тех, кто эти приемы применяет. Гениальность людей, придумавших стандартную схему англосаксонской операции ИВ, заключается именно в их способности выстроить из элементарных приемов грамотную тактическую комбинацию, заточенную на достижение конкретной цели.

Материалы, представленные в рамках второй главы, включены в программу подготовки руководящего состава Центрального аппарата МВД РФ и ряда других профильных ведомств.

Вместе с тем ничто так не закаляет человека, как практика. И ничто так не убеждает в правдивости любых слов, заключений и выводов, как возможность увидеть их действие в реальной жизни. Именно поэтому третья глава книги посвящена демонстрации (и в какой-то степени анализу) конкретных кейсов, примеров, иллюстрирующих схемы и технологии информационных войн в действии, одновременно раскрывая особенности планирования, организации и проведения информационных атак на первых лиц государства — «Дела об отравлении Сергея и Юлии Скрипалей», «Панамского досье», «Аргентинского кокаинового скандала», «Кремлевского доклада» Минфина США, вброса о «связи ИГИЛ и режима Асада», «беспрецедентной атаке ЦРУ» и др. На примере этих операций информационной войны, ведущейся против России, раскрываются особенности практического применения технологий фрейминга, якорения, «наклеивания ярлыков», «пробных шаров», операции «контролируемой утечки», технологии класса *WikiLeaks* и феномена Сноудена, технологии класса «Псаки — Мэтью Ли», применяемые в большой политике.

Важнейшей составляющей современных информационных войн России и США сегодня выступает миф о вмешательстве в президентские выборы. Он по своей природе зеркален:

- США обвиняют Россию (русских хакеров, курирующих их работников ГРУ ГШ ВС РФ и не только их одних) в прямом вмешательстве Кремля в выборы президента Соединенных Штатов в 2016 году, в результате которого «природный американский патриот» Хиллари Клинтон, замеченная в связях с ИГИЛ[1], с треском проиграла «правильному американскому националисту» Дональду Трампу, (якобы) сделавшему ставку на российские спецслужбы (*KGB*);
- Россия обвиняет Соединенные Штаты в прямом и неоднократном вмешательстве в президентские выборы в Российской Федерации, начиная с 1996 года.

[1] Террористическая организация «Исламское государство», запрещенная на территории Российской Федерации (*прим. автора*).

Если в случае с американской версией вмешательства России в президентские выборы в США-2016 в целом все понятно (это политический миф, основанный на манипулировании сознанием американских граждан путем использования предельно примитивных штампов типа «Трамп продался Кремлю», «Трамп — кремлевский наймит», «русские идут», «русские хакеры под каждой кроватью», «поскреби Трампа — найдешь Путина» и т.д.), то с российской версией все не так просто: в распоряжении руководства нашей страны есть факты, не просто подтверждающие факт вмешательства, но и детально раскрывающие тактику и стратегию, организационные и технологические схемы вмешательства США в президентские выборы в Российской Федерации в 1996, 2000, 2004, 2008, 2012 и 2018 гг. Именно этому посвящен доклад «Вторжение»[2], на базе которого в книге сформирована четвертая глава монографии.

Все эти методы и технологии вмешательства во внутренние дела РФ, представленные в четвертой главе, также используются в рамках операций информационной войны, но при этом имеют свои отличительные особенности в части планирования, выбора стратегии вмешательства, целеполагания и выбора главного и второстепенного объектов воздействия. При этом само вмешательство во внутренние дела Российской Федерации представляет собой ряд конкретных мер и действий, совершаемых зарубежными государствами с целью перехвата управления внутренними политическими процессами и политической деятельностью ключевых демократических институтов, включая институт выработки политических (управленческих) решений и институт демократических выборов в Российской Федерации, и осуществляется прямыми методами (посредством подкупа политических и общественных деятелей, финансирования и обучения оппозиции, скупки региональных СМИ), применением специальных технологий дестабилизации политической ситуации в стране и вовлечения населения в массовое протестное движение, направленное против действующей власти.

---

[2] Вторжение. Вмешательство США в выборы в Российской Федерации в ходе президентских кампаний 1996—2018 гг. М.: ЭИСИ, 2018. 32 с.

Подчеркивая практическую ценность и новаторство представленного в монографии научного подхода к исследованию проблем вмешательства иностранных государств во внутренние дела Российской Федерации, не лишним будет отметить, что материалы, представленные в рамках третьей главы настоящей книги, легли в основу формирования избирательной стратегии В.В. Путина в 2018 году.

Как говорил В.И. Ленин, «всякая революция лишь тогда чего-нибудь стоит, если она умеет защищаться»[3]. Если есть операции информационной войны — надо уметь им грамотно противодействовать. Иначе вас просто задолбают «вусмерть-не-по-детски», вопреки всяческим законам гуманизма, добра и красоты. В этом плане даже профессионалам и информационным киллерам лучше держаться вместе, наваливаться на продвинутого и весьма прошаренного противника скопом, а следовательно, объединяться в конгрегации с теми странами, которые испытывают сходные проблемы. В этом ключе наиболее перспективным выглядит создание межгосударственных союзов и блоков, заточенных на обеспечение коллективной информационной безопасности стран-участников — только так можно в современных условиях защитить себя от новейших американских операций и технологий информационной войны. Этим вопросам и проблемам объединения различных стран перед лицом общей опасности и посвящена следующая, пятая по абсолютному счету, глава монографии. В ней детально рассматриваются основные принципы и направления формирования единого пространства коллективной кибербезопасности стран БРИКС.

Цель создания такого пространства в современных условиях очевидна: организация совместного противодействия новым вызовам и угрозам в информационной сфере, таким как киберпреступность, информационный терроризм и экстремизм, операции информационной войны, с которыми каждая из входящих в БРИКС стран в отдельности не способна справиться. Поскольку реальные проблемы в плане обеспечения информационной безопасности и защиты от операций информационной войны есть у всех, даже у Китая, стремящегося отгородиться от этих угроз

[3] *Ленин В.И.* ПСС. Т. 37.

своими «золотыми щитами» и сравнительно недавно принятым новым законом о кибербезопасности 2016 года, копирующим так называемый «пакет Яровой». При всей высокой степени накачанности кибермускулатуры, у России, Китая, Индии, Бразилии и ЮАР по-прежнему остаются проблемы, связанные с обеспечением безопасности и защитой государственного суверенитета, которые в принципе невозможно решить на национальном уровне. Ярким примером этого остается Китай, многочисленные «золотые щиты» которого научились обходить ну все кому не лень, во-многом, благодаря существованию в составе КНР такого района как Гонконг, который, в силу специфичности своего статуса и истории происхождения, является для китайской партноменклатуры «великим всекитайским офшором», в том числе в информационной сфере.

Однако эти общие проблемы можно довольно быстро и эффективно решить, сформировав в БРИКС единую систему обеспечения и единое коллективное пространство информационной безопасности. При этом главным основанием для создания такого пространства и системы, обеспечивающей его информационную безопасность на уровне, отвечающем национальным интересам стран БРИКС, является общая для всех стран — участников этого объединения жизненно важная потребность в противодействии транснациональной киберпреступности и в отражении операций информационной войны, организуемых зарубежными противниками и конкурентами БРИКС.

Для эффективного функционирования надгосударственной системы обеспечения коллективной безопасности БРИКС в информационной сфере (включающей в том числе функции противодействия операциям информационной войны) необходимо создание наднациональной же системы органов, которые станут рабочим аппаратом, отвечающим за реализацию программ обеспечения коллективной безопасности БРИКС. Необходима собственная киберполиция БРИКС, работающая по принципу Интерпола, и много чего еще. Такая система может быть организована на основе опыта создания и функционирования соответствующих наднациональных органов Европейского союза.

Следует также отметить, что материалы, представленные в рамках пятой главы, легли в основу решений Совета безопасности Российской Федерации по формированию пространства коллективной кибербезопасности стран БРИКС, а также резолюций Научного совета при Совете безопасности РФ (в частности резолюции от 31 октября 2017 года).

Шестая глава учебного пособия посвящена цветным революциям и гибридным войнам — явлениям, очень близко расположенным к современным информационным войнам и во многом им родственным. В этом нет ничего удивительного: гибридные войны, так же как и войны информационные, относятся к одному и тому же классу противоборства — вооруженным конфликтам (различия между гибридной и информационной войной, помимо форм и методов ведения войны, состоят еще и в том, что информационная война носит узкоспециализированный, а гибридная — комплексный, сложносоставной характер); англосаксонские цветные революции роднит с англосаксонскими же операциями информационной войны то, что в основе и тех и других лежит одна-единственная организационная политическая технология. Действительно, если цветная революция — это технология организации государственных переворотов и демонтажа политических режимов, то психологическая операция — это тоже технология политической дестабилизации, которая может успешно применяться и для свержения действующей власти совместно с цветными революциями, а впоследствии — и в рамках начинающейся на обломках разрушенного государства гибридной войны. Но при этом важно совершенно отчетливо понимать, что информационная война, гибридная война, цветная революция и часто сопутствующая им в статьях мягкая сила — не одно и то же, это не синонимы, которые можно применять по отношению к реальным политическим процессам без должной степени осторожности и аккуратности. Так, цветные революции часто путают и с гибридными войнами, и с мягкой силой. А это неправильно, и в этом читатель сможет убедиться, прочитав пятую главу.

Помимо всего прочего, в этой главе представлена технологическая схема осуществления цветной революции, которая вызовет несомненный интерес как у специалистов, так и просто

у интересующихся данной политической проблематикой. А в одном из параграфов подробно — по шагам — расписана одна из реальных технологий конфликтной мобилизации молодежи, использующейся для вовлечения молодых людей в «цветное» протестное движение. Поле действия этой технологии — социальные сети, в которых активисты и политтехнологи цветных революций сначала создают социальные сообщества (группы) с сугубо неполитической повесткой (например, группы любителей персидских котят), а затем в несколько приемов меняют неполитическую повестку группы на политическую, а ее, в свою очередь, — на протестную, направленную против действующей власти. При этом изменения в повестке строятся таким образом, что они ускользают от внимания членов группы, и им кажется, что это они сами сделали выбор в пользу протестных настроений. А на самом деле ими умело манипулируют. Технология называется «Убить котенка».

Седьмая глава посвящена эволюции современного международного терроризма, террористического рекрутинга (форм и методов вербовки террористами молодежи) и проблемам борьбы с ним. Это довольно сложная тема: для того, чтобы эффективно бороться с современными сетевыми террористическими организациями, надо знать формы и методы их деятельности, особенности внутренней организации (т.е. их сетевую структуру), идеологию (у террористов она, безусловно, есть) и множество тонких моментов, деталей, особенностей, отличающих реальных террористов от их собирательного образа, присутствующего в научных статьях и публицистике. Необходимо также понимать, что единственный эффективный способ борьбы с современными сетевыми террористическими группировками — это агентурное внедрение в кадровый состав террористических группировок и создаваемые ими на захваченных территориях структуры военно-гражданской администрации. Ведь именно отсутствие агентуры в рядах террористов и крайне плохо поставленная агентурная работа французской контрразведки и стали настоящей причиной террористических актов в Париже, совершенных в ночь на 13 ноября 2015 года (взрывы на стадионе «Стад де Франс» в Сен-Дени и ряде других объектов, бойня в концертном зале «Батаклан»). При этом деятельность спецслужб по агентурному

проникновению в террористические организации должна сопровождаться отсечением террористов от каналов снабжения и источников поступления финансовых средств, без которых деятельность любой террористической группировки в принципе невозможна.

В главе содержится детальный анализ основных этапов и форм эволюции организационной структуры и принципов формирования террористических группировок, которая насчитывает четыре последовательных этапа (поколения), при прохождении которых они приобретали новые качества. Соответственно, сегодня в мире существуют и активно действуют организованные террористические группировки четырех различных поколений — от «Хезболлы» (группировки первого поколения) и «Талибана» (являющегося террористической группировкой второго поколения) до ИГИЛ (являющегося группировкой четвертого поколения). При этом каждое из поколений имеет свои отличительные особенности, которые были приобретены террористическими организациями именно в процессе линейной эволюции, восходящей от примитивных форм к сетевым структурам с претензиями на собственную квазигосударственность. При этом процесс террористогенеза в этой среде еще не окончен и в будущем следует ожидать появления на мировой арене новых форм существования террористических организаций, более опасных, чем все их предшественники.

Исследуя международный терроризм, нельзя пройти мимо идеологии террористов и их деятельности, связанной с организацией террористической пропаганды и распространением террористических «ценностей» в глобальном информационном пространстве (проявлениям «мягкой силы» террористов). Этим вопросам посвящен пятый подраздел седьмой главы, содержащий результаты сравнительного политологического анализа моделей «мягкой силы» сетевых террористических организаций на примерах ИГИЛ, «Аль-Каиды», «Талибана» и «Братьев-мусульман». При этом предметом рассмотрения в данном случае выступают формы, методы, модели и технологии «мягкой силы» данных террористических организаций. Современные террористы действительно широко используют в своей

идеологической и пропагандистской деятельности «мягкую силу» в целях сплочения, вовлечения в нее новых адептов и для ведения информационной войны со своими идеологическими противниками (как с правительствами различных стран, борющимися с международными терроризмом, так и со своими прямыми конкурентами из числа экстремистов, террористов и исламистов). При этом «мягкая сила» террористов не повторяет формы и методы «мягкой силы» США, известной нам по работам американских неолибералов (Дж. Ная, Р. Кохейна и др.), а имеет свою собственную модель, существующую в виде определенного набора версий, адаптированных под идеологию каждой конкретной международной террористической группировки: так, свои модели «мягкой силы» есть и у ИГИЛ, и у «Талибана», и у «Аль-Каиды», и у «Братьев-мусульман», и эти модели довольно сильно отличаются друг от друга даже в своей базовой основе.

В данном контексте не менее интересными представляются технологии террористического рекрутинга, применяемые террористами на постсоветском пространстве (в основном в странах Центральной Азии), детально описанные в шестой части седьмой главы, и технологии вербовки террористами адептов в социальных сетях, изложенные в седьмой части той же главы. В этом плане следует отметить прекрасную методологию и авторский научный подход И.С. Шегаева, результаты исследований которого легли в основу сначала совместной статьи, а затем и раздела, посвященного террористическому рекрутингу в ЦА[4]. Что касается раздела, посвященного технологиям вербовки, то этот материал первоначально был написан сугубо в практических целях — в интересах судебной экспертизы, по заказу Межрегионального бюро судебных экспертиз имени Сикорского[5]. Теперь, по прошествии определенного времени, появилась

[4] См.: *Манойло А.В., Шегаев И.С.* Террористический рекрутинг на постсоветском пространстве: современные тенденции и риски для России // Вестник Московского государственного областного университета (Электронный журнал). 2018. № 2. DOI 10.18384/2224-0209-2018-2-880.

[5] См.: *Манойло А.В.* Криминализация информационного пространства и преступная деятельность экстремистских группировок в социальных сетях [Электронный документ] / Межрегиональное бюро судебных экспертиз имени Сикорского. URL: https://www.expertsud.ru/content/view/207/36/ (дата обращения: 20.07.2018).

возможность, наконец, ознакомить с ним массового читателя. При этом стоит отметить, что за два года, прошедших с момента его создания, формы и методы вербовочной деятельности террористов в социальных сетях принципиально нисколько не изменились.

Благодарности

Мы выражаем искреннюю благодарность доценту И.С. Шегаеву за прекрасный концептуальный анализ и глубокие научные выводы, вошедшие в раздел седьмой главы «Террористический рекрутинг: индексы, формы, методы, технологии»; аспирантам МГУ имени М.В. Ломоносова Б.Б. Лавринову и Н.В. Авдеевой, внесших большой вклад в подготовку доклада «Вторжение» (материалы которого сформировали четвертую главу) и в формирование облика концепции кибербезопасности БРИКС; моим ученикам, аспирантам МГУ имени М.В. Ломоносова А.В. Курилкину и И.И. Валиуллину, материалы которых легли в основу раздела «Эволюция понятий и представлений об информационной войне» второй главы; журналисту К. Стригунову, в соавторстве с которым написан заключительный параграф третьей главы «Ставки в игре растут: в Венесуэле может готовиться верхушечный переворот»; доценту Ф.О. Трунову, выдающемуся ученому-международнику, германисту, за корректуру содержания пятой главы (в части, касающейся кибербезопасности БРИКС) и насыщение ее полезной фактурой.