ВВЕДЕНИЕ

Книга, которую Вы, уважаемый читатель, держите сейчас в руках, посвящена информационным войнам и психологическим операциям, из которых эти самые войны состоят, напоминающим детали конструктора. И ничему другому. Кроме того, в этой книге, помимо сведений об информационных войнах, Вы обязательно найдете еще множество всякой всячины, которую должен знать специалист в этой области. Многие из этих знаний (например, оперативное внедрение в рейдерские организации или наружное наблюдение, операции контролируемой утечки или вербовочная уязвимость) относятся даже не к области научных знаний, а к описанию ремесла, которым владеют разведчики.

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 бешенный 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. Поймал этот момент, нанес один филигранно просчитанный, чрезвычайно точный удар — и все, можно до конца месяца на работе ничего не делать. Просто лежать на диване и плевать в потолок. Мечта опера, следовать которой я стремлюсь по жизни. Заманчиво? Вот и я о том же.

Путь к истине иногда бывает тернист и запутан. В этой книге сделана героическая попытка его спрямить — настолько, насколько вообще это возможно в такой непростой и чрезвычайно запутанной области знаний, как информационные войны и психологические операции. Сделать это непросто: еще минуту назад тебе казалось, что выбранный тобой азимут — правильный, и компас вроде не барахлит, и бензина в наручных часах еще полбака, а спустя всего несколько минут ты забираешься в такие дебри, в которых успел побывать до тебя только бравый солдат Швейк, анабазис которого надлежащим образом задокументирован Ярославом Гашеком. Проходит еще одна минута — и ты уже сам становишься Швейком.

К моему смущению, я не очень хорошо знаю Гашека. А уж с его солдатом Швейком вообще лично не знаком. Судя по обрывочным сведениям, Гашек — это, вероятно, военный командир (может быть даже красный), раз у него есть свой персональный солдат. Мотаться по разным местам, таская за собой солдат, — это вообще свойственно всем военным, особенно их командному звену: достаточно вспомнить Дона Кихота, который повсюду таскал за собой Санчо Пансу, без всякой видимой пользы, а так, отдавая дань традиции. Швейк, часто упоминаемый в народном фольклоре, — это, скорее, собирательный образ, вобравший в себя индивидуальные качества личностей из какой-нибудь

полуроты гренадер. Известно лишь одно: знаменитый путь Швейка на фронт, пролегавший через все пивные кабаки и из-за этого названный «анабазисом», несомненно, имеет греческое происхождение. Анабазис — греческое понятие (авторство этого слова, в свою очередь, приписывают Ксенофонту). Следовательно, Швейк наверняка грек, причем — древний (это вам не коньковый бег; анабазисом ходили исключительно в эпоху греко-персидских войн), и вероятно, упоминания о нем следует искать в «Одиссее» Гомера (так как именно она повествует об исключительно запутанных скитаниях и о том, что древние греки прямых путей не искали, как на фронт, так и с фронта). Возможно разобраться в этом поможет первоисточник (*Гашек Я.* «Похождения бравого солдата Швейка»), а может, автор пишет совсем не о том Швейке. И Гашек этот какой-то не тот. Но традиции анабазиса продолжают в нас жить, следуя уже не греческой, а чисто славянской народной мудрости, гласящей, что «русские витязи прямыми путями не ходят».

Именно поэтому данная книга начинается не с обсуждения информационных войн (то есть, с извечных вопросов, волнующих человечество на протяжении многих веков: «что сие гой если?» и «откель пошла есть 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, то есть — 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 хитросделанным 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 Метью 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 информационной войны (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-Метью 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.

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

[1] Террористическая организация «Исламское государство», запрещенная на территории Российской Федерации. — *Прим. автора.*

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»[1], 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), и применением специальных технологий дестабилизации политической ситуации в стране и вовлечения населения в массовое протестное движение, направленное против действующей власти.

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 великий Ленин, «всякая революция лишь тогда чего-нибудь стоит, если она умеет защищаться»[2]. Если есть операции информационной войны — надо уметь им грамотно

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

[2] Ленин В.И. ПСС. Т. 37.

противодействовать. Иначе вас просто задолбают «в усмертьне-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 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, отвечающим 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 монографии 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, также 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 у просто 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 (то есть 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 4 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 Хезбаллы (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 Центральную Азию (ЦА)[1]. 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

[1] 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.

экспертиз имени Сикорского[1]. Теперь, по прошествии определенного времени, появилась 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.

Сфера информационных войн и психологических операций — это область применения инструментов информационно-психологического воздействия, коммуникационных технологий. Специалист ведения информационных войн по определению должен быть отличным коммуникатором, владеть специальными техниками, позволяющими просчитать соперника или партнера, его действия на много шагов вперед, тем самым обеспечив себе конкурентное преимущество, даже еще не вступив в схватку. В этом плане овладеть современными техниками эффективной коммуникации читателю поможет восьмая глава. В ней содержится описание базовых подходов к расширению личного коммуникационного ресурса специалиста в сфере ИВ (модальности и техники их определения, тонкая настройка на «волну» партнера по коммуникации, исходя из знания его модальности), описание техник считывания невербальных сигналов партнера по переговорам по движению глаз (т.н. «глазные сигналы доступа»), а также техника публичных выступлений в СМИ, особенности формирования плана публичного выступления, ведения полемики во время спора и анализ ошибок человека, выступающего публично, психологические уловки в споре и методы их нейтрализации. Следует отметить, что данная глава в чистом виде является практическим руководством для коммуникатора и переговорщика, позволяя использовать изложенные в ней техники с ходу, «с колес»; академизм в ней, увы, сведен к исчезающе малой величине. Однако именно это и будет привлекать практикующих специалистов, для которых глава станет прямым руководством к действию и, одновременно, калибровочным инструментом. Если надоело разбираться в теории мироздания — переходите прямо к восьмой главе и, ручаюсь, ни разу не пожалеете.

1 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).

Материал, изложенный в восьмой главе, написан в соавторстве с профессором А.И. Петренко по заказу Всероссийской политической партии «Единая Россия» (в рамках существовавшего в ней прежде федерального партийного проекта «Гражданский университет»). Основанные на этом материале методические рекомендации использовались в партийной учебе высшего руководства ЕР — руководства фракции ЕР в Госдуме ФС РФ, депутатов ГД и законодательных собраний регионов РФ, сенаторов, руководителей региональных отделений и их заместителей по агитационно-пропагандистской работе, и неизменно пользовались популярностью. Насколько при этом владение этими техниками помогло бывшим и нынешним депутатам в их дальнейшей карьере, доподлинно неизвестно. Но можно предположить, что у функционеров ЕР и с этими знаниями, и без этих знаний и так все хорошо.

При прочтении восьмой главы может показаться, что все представленные в ней техники и методики относятся к разряду нейро-лингвистического программирования (НЛП). В этом плане могу заверить Вас со всей определенностью: не все. Основной объем знаний в этой области почерпнут в годы учебы в одном довольно известном специальном учебном заведении, а затем отшлифован годами практики и жизненным опытом. Как именно называется это загадочное учебное заведение? Пусть это останется за рамками книги. Достаточно знать, что оно и сейчас существует и прекрасно себя чувствует.

Девятая глава монографии посвящена деятельности рейдеров — рейдерским захватам и корпоративному шантажу (более известному в криминальной среде как «гринмейл»), а также формам и методам борьбы с этим видом организованной преступной деятельности. В главе пошагово описаны две основные схемы рейдерских захватов — первичного и повторного (вторичного), — включающие детальную характеристику всех этапов подготовки, разведки и предварительной подготовки захвата, организации «силового входа», взаимодействия рейдеров с отдельными коррумпированными представителями местной администрации и правоохранительных органов, специальных служб. Глава содержит описание и характеристику структуры рейдерского холдинга, включая функционал отдельных его «дочерних предприятий»; принципы организации работы разведки и контрразведки рейдеров (как технической, так и агентурной), в том числе подразделений, отвечающих за собственную безопасность; характеристику психологических портретов высшего

руководства рейдерских организаций (включая руководителей блоков и управлений внешней и внутренней безопасности). Отдельное внимание уделяется вербовочной уязвимости рейдеров и каналам как оперативного, так и агентурного проникновения в кадровый состав рейдерских организаций.

Десятая глава монографии содержит два очерка о жизни разведчиков службы наружного наблюдения Норвегии и Украины. Оба материала описывают реальные случаи из жизни, заметно контрастируют друг с другом и, в целом, описывают жизнь разведчиков, подцепивших «хвост», такой, какая она есть — без романтики и героизации. Это, конечно, уже не научная работа, а литературное «хулиганство». Но и в этом хулиганстве читатель, уверен, найдет для себя много любопытного и, даже может, полезного. Работники спецслужб, действующие или бывшие, увидят в этих историях детали, которые, может быть, были и в их личной практике, и улыбнутся. Обычные же граждане, не знакомые с работой спецслужб на своем личном опыте (и слава святой сосиске!), смогут сравнить уровень работы служб наружного наблюдения в различных странах и одновременно убедиться в том, что очень многое в работе разведчика определяется даже не опытом, а просто обыкновенным везением.

Наконец, заключительная одиннадцатая глава монографии посвящена политическим портретам лидеров, политический стиль которых автору доводилось анализировать в интересах дела. Кто они — узнаете, прочитав одиннадцатую главу.

На этом, к сожалению, все. Для полноты ощущений и поддержания баланса Вселенной в удовлетворительном состоянии следовало бы еще написать о коррупции, которую многие причастные к этому явлению (со стороны коррупционеров, конечно) считают не опасной болезнью общества, а, наоборот, «двигателем прогресса». Но об этом мы напишем в нашей следующей книге.

Благодарности

Мы выражаем искреннюю благодарность выдающемуся психологу и политологу, профессору А.И. Петренко, в соавторстве с которым написаны материалы, составившие в книге восьмую главу («Техники эффективной коммуникации»); профессору И.К. Мельнику за предоставленный материал по разделу «Психологические уловки в споре» (включенному в восьмую главу настоящей книги); доценту И.С. Шегаеву за прекрасный концептуальный анализ и глубокие научные выводы, вошедшие в раздел

седьмой главы «Террористический рекрутинг: индексы, формы, методы, технологии»; прекрасные и высокопрофессионально составленные главным редактором журнала «Деловой ключ» материалы интервью «Эволюция терроризма», включенные в седьмую главу данной книги в формате первоисточника; 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; доценту Ф.О. Трунову, выдающемуся ученому-международнику, германисту, за корректуру содержания пятой главы (в части, касающейся кибербезопасности БРИКС) и насыщение ее полезной фактурой.