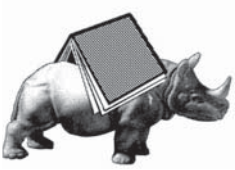

КИБЕРВОЙНА И КИБЕРМИР РИЧАРДА КЛАРКА

Cyberwar. The Next Threat to National Security and What to Do About It. By Richard A. Clarke and Robert K. Knake. Ecco. 290 p.

Рецензия — Олег Демидов

Ричард Алан Кларк проработал с госструктурах США ни много ни мало 30 лет, с 1973 по 2003 г. — сначала в Пентагоне и Госдепартаменте США, а позже в Совете национальной безопасности США. На последнем месте службы он в разное время занимал должности руководителя Группы по обеспечению контртеррористической безопасности, специального советника и, при администрациях Билла Клинтона и Джорджа Буша-младшего с 1998 по 2001 г., пост Национального координатора по безопасности, защите инфраструктуры и контртерроризму. На посту Национального координатора особое внимание г-н Кларк уделял кибербезопасности, включая проблемы кибершпионажа и конфликтов в киберпространстве. Затем, в силу глубоких разногласий с курсом Буша в сфере национальной безопасности, ушел, как водится, в частный сектор. А в 2010 г., в соавторстве с молодым исследователем Робертом Кнейком, написал книгу *Кибервойна. Новая угроза национальной безопасности и пути ее преодоления*, вложив в нее весь свой опыт и все знания, приобретенные за долгие годы госслужбы.

То, что получилось, можно назвать одной из наиболее системных, всеобъемлющих и практических публикаций на тему военно-политического значения киберпространства, в первую очередь для США. Книга идеальна для тех, кто желает вникнуть в проблематику кибервойн на серьезном уровне с нуля, не будучи специалистом в этой области. Авторам удается сочетать доступную и легкую манеру изложения с въедливым анализом нынешней ситуации и богатейшей фактурой. Место находится даже элементам академической теории, вплетаемым в рассуждения о сходстве нынешней эпохи с 1950-ми гг., когда военный атом, так же, как и кибероружие сегодня, поставил мир перед задачей выработать режим его контроля во избежание глобальной катастрофы.

Кларк показывает проблему в полном ракурсе, начиная с описания того, что такое кибервойна, насколько она реальна и какие события в недавнем прошлом можно считать ее первыми прецедентами. Стоит ли отсчитывать ее историю от кибератак против государственной и коммерческой инфраструктуры Эстонии, сопутствовавших скандалу вокруг *Бронзового солдата* в 2007 г.? Или от подобных, но еще более масштабных атак на инфраструктуру Грузии, впервые происходивших параллельно с военным конфликтом — *Пятидневной войной* в августе 2008 г.? А что, если понятие кибервойны подразумевает поражение военных систем, напрямую влияющее на *оффлайновое* пространство боевых действий? В таком случае счетчик истории кибервойн возвращает нас в 2007 г. к операции *Фруктовый сад*, когда бомбардировке сирийского объекта, предположительно связанного с подпольной ядерной программой, предшествовал взлом систем ПВО Сирии при помощи компьютерной программы *Senior Suter*. Авторы разбирают каждый пример с технической изнанки, давая читателю редкий по емкости и четкости анализ инструментария кибервойн — от примитивных DDoS-атак и типовых *логических бомб* до сверхсложных червей, выводящих из строя промышленное оборудование, и программ, позволяющих *ослеплять* современные системы ПВО.

Оставляя ответ на усмотрение читателя, Кларк озадачивает его очередным вопросом — если кибервойна реальна, кто же ее ведет? Ничтоже сумняшеся, объявляя РФ основным *дирижером* и организатором атак на Грузию и Эстонию, авторы все же признают и подробно рассматривают *проблему атрибуции* — одно из ключевых препятствий к предотвращению кибервойн. Несмотря на это, в фокусе внимания оказываются не анонимные хакерские группировки или кибертеррористы — последним в книге почти не отводится места, что вообще симптоматично с учетом послужного списка Кларка, — а государственные или квазигосударственные структуры.

В главе *Кибервоины* дается прекрасный обзор того, как в американских госструктурах на организационном уровне оформлялась повестка военно-стратегической кибербезопасности. В 2009 г. этот процесс увенчался созданием Киберкомандования, но отнюдь не закончился. Кларк дарит читателю отличную возможность проникнуть в лабиринты межведомственной борьбы за контроль над военной киберповесткой в американских спецслужбах и армии. Где еще можно из первых рук узнать подноготную затяжного *перетягивания каната* между киберподразделениями ВМС, ВМФ и Сухопутных сил США? Вникнуть в суть дискуссии о том, на каком структурном уровне должна была быть обособлена кибероборона — от 10-го флота в составе ВМС (или субструктуры ВВС) до нового *вида* войск — и насколько причудливым и гибким компромиссом в этом смысле стало Киберкомандование в его нынешнем виде?

Вслед за США анализируется КНР с многоуровневой системой всевозможных сообществ, ведущих борьбу в киберпространстве в интересах Поднебесной и в различной степени связанных с государством. На вершине этой пирамиды находятся секретные штатные киберподразделения НОАК, в основании — обычные китайские граждане, которые нередко выражают свои патриотические чувства, участвуя в DDoS-атаках на ресурсы государств или компаний, навлекших на себя гнев Пекина. В середине же этой сложной иерархии — масса университетов, исследовательских центров и иных окологосударственных учреждений, полурегулярных ассоциаций и группировок сетевых активистов и патриотичных *кибервоинов*, которых трудно сосчитать. На фоне подробного анализа структур кибероборонны (и, в не меньшей степени, кибернападения) немного теряется Россия, в отношении которой познания авторов заканчиваются на Федеральном агентстве правительственной связи и информации при Президенте РФ (ФАПСИ), упраздненном в 2003 г., а также расплывчатом упоминании Главного разведывательного управления и Службы внешней разведки. Что ж, для российских спецслужб столь скудные познания о них американских коллег могут считаться и поводом для гордости.

Глава 3, *Поле битвы*, посвящена рассмотрению того, где, в каких сетях ведется или, скорее всего, будет вестись кибервойна и какие свойства сетей делают кибервойну не только реальной, но и весьма вероятной уже сегодня. Авторы рассматривают особенности и уязвимость интернета, связывающего воедино изолированные островки киберпространства. Уязвимость Сети делает возможным перехват информации, ее изменение, удаление, нарушение работы глобальной системы доменных имен (DNS) и, в конечном счете, разрушение целостности киберпространства. Все это позволяет авторам говорить о том, что в кибервойне интернет может выступать как основным пространством и *каналом* для агрессивных действий, так и их конечной *целью*. При этом в мире развивается процесс усиления зависимости промышленных, военных и иных критических технологий от информационных систем. Компьютеры и сети необходимы для функционирования современной финансовой системы, транспортной и энергетической логистики всех видов, энергогенерирующих и энергораспределительных систем и, конечно, передовых военных разработок.

По большинству параметров США являются наиболее зависимой от кибертехнологий нацией в мире, вплоть до того, что оптимизация промышленных процессов требует подключения автоматизированной системы управления технологическим процессом (АСУ ТП) не просто к локальным сетям, а к интернету, а соединения войск, унаследовавших парадигму *сетецентричности* от администрации Буша-младшего, при нарушениях сетевых коммуникаций теряют боеспособность. Особым *пунктом,* на который авторы раз за разом делают упор, является уязви-

мость энергосетей и генерирующих мощностей, в основном находящихся в частной собственности. Кларку явно неуютно от того, что возможности федерального регулирования, которое повысило бы стандарты кибербезопасности на объектах энергосистемы США и обязало операторов изолировать АСУ ТП от интернета (или хотя бы должным образом шифровать управление энергомощностями), ограничены и наталкиваются на неизменное сопротивление лоббистских группировок. Между тем, именно информационные системы энергосетей и генераторов на электростанциях стали самым лакомым куском для китайских и прочих хакеров, которые уже напичкали их *потайными входами* и *логическими бомбами*, отследить и обезвредить которые полностью невозможно.

Это обусловливает несопоставимую с потенциальными противниками уязвимость США в случае кибервойны. Одна из главных задач, которую ставит перед собой Кларк — донести до Белого дома, Пентагона, а заодно и массовой аудитории тезис о том, что высокий уровень развития ИКТ может стать для США *ахиллесовой пятой* в случае конфликта. При этом превосходящий потенциал *кибернападения*, которое грозит превратиться в *доктринальный фетиш* в стенах Пентагона, не компенсирует уязвимость и зачастую нивелируется меньшей зависимостью потенциальных противников от киберинфраструктуры. Любопытной, хотя и небесспорной иллюстрацией парадоксов потенциала государств в киберпространстве служит таблица, приводимая Кларком в главе 5, *На пути к стратегии обороны*. Для того чтобы сопоставить потенциал США и их вероятных противников в кибервойне (КНР, РФ, Ирана и КНДР), вводятся три равновесных показателя — потенциалы кибернападения и кибероборонs, а также степень зависимости национальной инфраструктуры и экономики от кибертехнологий. В итоге США уступают всем вероятным оппонентам, а высший балл получает... КНДР, несмотря на довольно слабый наступательный киберпотенциал. Такая оценка парадоксальна, но справедлива в том смысле, что разрушение примитивной киберинфраструктуры КНДР, во-первых, никак не скажется на экономике и военной мощи страны, а во-вторых, не компенсирует тот ущерб, которые вражеские *кибервоины* теоретически могут нанести США.

А на описание последствий кибервойны для США Кларк с коллегой не скупятся, рисуя поистине апокалиптическую картину: взрывы на химических заводах и токсичные облака над мегаполисами, пожары на нефтехранилищах и трубопроводах, транспортный коллапс на дорогах и в аэропортах. Нация оказывается буквально парализована без электричества, управления, защиты и информации о том, что происходит. Пожалуй, Кларка можно упрекнуть в алармизме и преувеличении рисков такого сценария. В нем все же говорит чиновник, чье видение информационных технологий много лет формировалось сквозь призму исходящих от них угроз. Однако в кейсе о киберконфликте США и КНР в недалеком будущем (сюжет, уже ставший *sine qua non* в публикациях американских стратегов на тему кибервойн), авторы рисуют довольно сдержанный сценарий. Стороны обмениваются взломами секретных военных сетей, локальными *блэкаутами* в нескольких регионах, выводом из строя спутниковых коммуникаций и транспортной логистики. Человеческие жертвы отсутствуют или минимальны. И хотя США терпят поражение, для мира история скрыта за завесой дипломатических маневров, позволяющих Вашингтону худо-бедно сохранить лицо.

Чего же хотят авторы от нынешних хозяев Белого дома и адресован ли их труд только американскому политическому истеблишменту? Нет, не только — Ричард Кларк рискует углубляться в тему международно-правового регулирования поведения государств в киберпространстве, и это, пожалуй, наиболее ценная и актуальная для российского читателя часть *Кибервойны*. Если бы книга состояла лишь из главы *Кибермир*, полностью посвященной проблемам создания международного режима предотвращения кибервойн и регулирования применения кибероружия, она все равно стала бы одной из выдающихся публикаций на тему кибербезопасности за последние годы. В начале главы Кларк невзначай признается: именно он от лица США *зарубил* первые инициативы РФ по созданию международного режима предотвращения информационных войн, озвученные на площадке ООН еще в 1998 г., и продолжал блокировать их до ухода с госслужбы. Впрочем, заложенный

им курс был сохранен и после 2003 г. и до последнего времени поддерживался без сколько-нибудь существенных изменений.

В чем же дело? Кларк не стесняется называть российские инициативы пропагандой, лишенной реального содержания и направленной скорее на саботаж международного взаимодействия. Издание, правда, вышло до того, как осенью 2011 г. РФ презентовала концепцию Конвенции об обеспечении международной информационной безопасности, а четыре государства — члена ШОС, включая РФ и КНР, направили Генсеку ООН письмо с проектом Правил поведения в области международной информационной безопасности. Однако можно смело утверждать, что тональность г-на Кларка вряд ли существенно изменилась бы. Конечно, утверждения о пропагандистском характере российских предложений, как минимум, спорны и невольно вызывают желание обвинить автора в тенденциозности, тем более что не подкрепляются сколько-нибудь серьезными аргументами. По размышлении над прочитанным кажется, что проблема вовсе не в этом и на самом деле для США неприемлем *всеобъемлющий подход*, заложенный в основу инициатив Москвы. По мнению авторов *Кибервойны*, какое-либо комплексное соглашение ведущих мировых держав об отказе от ведения кибервойн — не говоря уже про кибершпионаж, а также от разработки кибероружия попросту невозможно, так как не подлежит эффективному контролю и не обеспечивается достаточными стимулами. Исходя из такой логики предложения и меры, составляющие суть российских инициатив, действительно неприемлемы для США.

Насколько Кларк прав *в этой части* — вопрос для отдельного большого исследования, но некоторые меры из числа названных в книге заслуживают внимания. В том числе, идея начать строительство международного режима кибербезопасности с точечных соглашений об ограничении либо запрете инициированных государствами кибератак на отдельные системы и объекты. Например, такие как информационная инфраструктура глобальной финансовой системы, от которой равно зависимы США, КНР, Россия и даже Иран. Сюда же напрашивается еще один перечень таких объектов, о котором Кларк лукаво умалчивает, несмотря на наличие в переиздании книги подробного комментария о черве *Stuxnet*. Почему бы не включить в такое соглашение инфраструктуру объектов, связанных с оружием массового уничтожения (ОМУ), и особо опасных *чувствительных* промышленных объектов, таких как АЭС, химические заводы и т. п.? Среди прочих идей авторов — соглашение о неприменении кибервооружений первыми даже в случае конфликта с использованием обычных вооружений, запрет атак на гражданскую инфраструктуру, включая в первую очередь энергосети.

Ключевая идея подхода, изложенного на страницах книги, — не пытаться добиться полного запрета кибервойн *с нуля*, из сегодняшнего состояния, близкого к анархии, а пошагово *взращивать* режим безопасности киберпространства, фиксируя и понемногу расширяя минимальные точки совпадения интересов основных игроков на международной арене. Кларк не случайно так часто и упорно ссылается на опыт режима контроля над ядерными вооружениями, который в основном сложился за время холодной войны. Тот режим формировался более 30 лет, и его развитие не завершилось до сих пор, как показывают яростные дискуссии вокруг глобальной ПРО США и ядерной программы Ирана. И начинался он с малого — например, с временного соглашения между СССР и США об ограничении стратегических наступательных вооружений (ОСВ-1), договоров о запрещении испытаний ядерного оружия в отдельных средах. Потребовались десятилетия с момента создания атомной бомбы и острейший Карибский кризис, прежде чем стороны перешли к вопросам *сокращения* ядерных арсеналов и перестали рассматривать нанесение массированных ядерных ударов по противнику в качестве реально применимого внешнеполитического инструмента. В эпоху кибертехнологий время течет несравнимо быстрее, однако база для режима безопасности киберпространства все же должна вызреть, вырасти из локальных соглашений и ограниченного консенсуса по отдельным вопросам.

По крайней мере, так считают авторы *Кибервойны*. Правы они или нет, судить читателю, в том числе и российскому. Но для этого труд Ричарда Кларка и Роберта Кнейка должен обязательно попасть на наши книжные полки — он того заслуживает.