Бедрицкий Александр Владимирович*, кандидат политических наук, старший научный сотрудник, заместитель начальника отдела евроатлантических исследований РИСИ.

Старые идеи для нового пространства[1]

В Соединённых Штатах вопросы противоборства в кибернетическом пространстве проработаны довольно хорошо. Практически каждый год выпускаются серьёзные исследования, посвящённые этой проблеме. В их ряду можно назвать монографии Дж. Карра "Кибервойна изнутри"[2], а также Р. Кларка и Р. Нейка "Кибервойна: следующая угроза национальной безопасности и что с ней делать"[3]. Более того, многие теоретические наработки получают своё практическое воплощение. Тема обеспечения безопасности киберпространства и ведения в нём боевых операций является одной из приоритетных для американской администрации. Об этом свидетельствуют постоянный интерес президента Б. Обамы к данной проблематике, публикация ряда официальных документов, регламентирующих государственную "кибернетическую" политику США, а также создание в Пентагоне профильных командований, включая объединённое командование кибернетических операций.

На этом фоне опубликованная в 2009 г. монография М. Либики "Киберсдерживание и кибервойна" вполне могла бы затеряться, пополнив и без того внушительный список теоретической литературы по данному вопросу. Тем не менее есть ряд причин, по которым рассматриваемая книга заслуживает большего внимания. Во-первых, М. Либики, является одним из "патриархов" концепции информационной войны. Его работа "Что такое информационная война" (What Is Information Warfare), опубликованная ещё в 1995 г., во многом не потеряла своей актуальности и сегодня, а обозначенные в ней направления информационного противоборства, хотя и переосмысленные, получили практическое развитие. Во-вторых, по мере перехода проблематики в практическую плоскость специалисты уделяют всё больше внимания не тому, *что*, собственно, представляет собой противоборство в киберпространстве, а то, *как* оно осуществляется. Книга М. Либики позволяет задуматься о применимости законов ведения войны к киберпространству, возможности осуществления стратегии сдерживания потенциального агрессора, а также о перспективах заключения международных договоров, ограничивающих военное использование информационных систем. Ну и, наконец, в-третьих,

* a.bedritsky@yandex.ru.

[1] Рецензия на книгу: *Libicky M. C.* Cyberdeterrence and Cyberwar / Martin C. Libicki. RAND Corporation, 2009. 214 p.

[2] *Carr J.* Inside Cyber Warfare / Jeffrey Carr. O'Reilly Media, 2010. 200 p.

[3] *Clarke R., Knake R.* Cyber War: The Next Threat to National Security and What to Do About It / Richard A. Clarke, Robert Knake. HarperCollins Publ., 2010. 294 p.

в российской публицистике понятия "информационная война" и "война в киберпространстве" в значительной степени мифологизированы, а книга М. Либики даёт представление о взглядах, существующих в США, и сложившейся практике, обрисовывает дальнейшие перспективы развития теоретической мысли и практических шагов в данном направлении.

М. Либики исходит из того, что киберпространство[4] – это самостоятельная среда с присущими ей правилами и законами. Например, успех кибероперaций определяется не столько развитием "наступательного потенциала", сколько поиском и использованием уязвимостей в информационных системах противника. В киберпространстве можно установить, откуда именно производится сетевая атака, но сложно выяснить, кто её осуществляет и зачем. Критическая зависимость современного общества от стабильности работы информационных систем в гражданской и военной сферах превращает кибератаки в самостоятельный вид боевых действий в пространстве, к которому традиционные военные стратегии и стратегии сдерживания не вполне применимы[5].

Осмыслению этих вопросов и поиску ответов на них и посвящена монография М. Либики. Особый интерес книге добавляет то обстоятельство, что она представляет собой результат исследования, проведённого по заказу ВВС США, которые на протяжении долгого времени претендовали на роль лидера в вопросах ведéния информационных и кибернетических операций.

Прежде всего, М. Либики задаётся вопросом, что такое кибератака? По его мнению, целый ряд действий, которые обычно принято относить к категории компьютерных атак (скажем, несанкционированный доступ к информации), таковыми вовсе не являются, как и традиционный шпионаж не является актом войны[6]. Из этого следует, что поиск адекватного и пропорционального ответа на такие действия затруднителен. Например, любое государство может объявить направленную против него кибератаку актом войны, но едва ли сможет предпринять ответные меры, которые все члены международного сообщества воспримут однозначно, а значит, само же выступит в роли агрессора[7]. Это обстоятельство делает сомнительным применение стратегии сдерживания в киберпространстве, несмотря на кажущуюся привлекательность использования принципов этой стратегии в информационной сфере. Основными причинами для такого скептицизма являются невозможность установить агрессора (было ли это государство, группа лиц или конкретный человек); предсказать, будут ли ответные действия восприняты агрессором как серьёзная угроза; и, наконец, разработать модель ведéния войны в киберпространстве[8].

С другой стороны, вслед за предпринятой кибератакой (против военных и сопряжённых с ними информационных систем), которая значительно

---

[4] Условное (*виртуальное*) пространство, образующееся в результате использования электронных и электромагнитных средств хранения, обработки и обмена данными в компьютерных сетях и связанных с ними инфраструктурах (см.: The National Military Strategy for Cyberspace Operations. Washington D.C., 2006. P. IV).

[5] *Libicky M. C.* Op. cit. P. 5–7.

[6] Ibid. P. 26.

[7] Ibid. P. 180.

[8] Ibid. P. 40.

снизит оборонный потенциал государства, может последовать традиционное военное нападение. В качестве примера М. Либики приводит гипотетический сценарий развития китайско-тайваньского конфликта, согласно которому перед вторжением будет проведена серия кибератак, направленных против информационных систем Тайваня. Их будет сложно однозначно увязать с действиями КНР, а значит Соединённые Штаты, выступающие гарантом безопасности острова, могут оказаться не в состоянии реагировать на них[9].

М. Либики также напоминает об одном из первых организованных кибернетических нападений – серии DDOS-атак против официальных эстонских сайтов, предпринятых после решения руководства этой страны о переносе "Бронзового солдата" из центра Таллина, указывая на полное отсутствие прямых свидетельств причастности к данным событиям официальной Москвы[10]. Тогда эстонской министр иностранных дел У. Пает возложил вину за эти кибераакции на Россию и обратился к руководству Североатлантического альянса с запросом о необходимости разбирательства этого дела и применимости положения ст. 5 Устава НАТО о коллективной обороне.

Казалось бы, пишет М. Либики, складывается безвыходная ситуация: даже очевидность угрозы не даёт возможности применить традиционный набор средств защиты. *Дипломатическое давление* в этом случае бессмысленно, поскольку сложно доказать факт угрозы, даже идентифицировав её источник. *Политика сдерживания*, основанная на угрозе применения силы, – нереализуема, поскольку потенциальным агрессором может оказаться не только государство, но и отдельные неправительственные группировки или даже частные корпорации, до которых невозможно донести соответствующим образом сформулированную угрозу возмездия и условия, при которых она будет осуществлена. *Непосредственно военное реагирование* на кибератаки возможно лишь при превышении некоего "болевого порога" систем жизнеобеспечения государства – объекта атаки, в противном случае это будет расценено как непропорциональное использование силы.

Всё это приводит автора к довольно нетривиальной мысли: если невозможно реализовать ясно выраженную политику сдерживания, то в ряде случаев вполне допустимо осуществить акт тайного возмездия. Иными словами, М. Либики всерьёз рассматривает возможность применения принципа "око за око".

В целом продуманная и в то же время смелая и откровенная позиция автора заслуживает самого пристального внимания и уважения. В частности, становится более понятным, каким образом будет осуществляться "активная кибероборона" (т.е. оборона, подразумевающая ведение наступательных действий), провозглашённая командующим кибернетического командования США К. Александером в качестве одного из принципов военной стратегии для киберпространства[11].

---

[9] *Libicky M. C.* Op. cit. P. 81.

[10] Ibid. P. 3.

[11] *Alexander K. B.* Statement of Commander United States Cyber Command Before the House Committee on Armed Service. Washington DC, US Congress. September 23, 2010.

Книга М. Либики позволяет также несколько иначе взглянуть на перспективы международных договорённостей и некоторые американские инициативы в кибернетической сфере. Надо отметить, что сам автор крайне скептически оценивает возможность достижения каких-либо международных соглашений в этой области, подобных договорам о контроле над вооружениями. Даже в том случае, если страны официально признают кибервойны угрозой международной безопасности (максимум, на что можно рассчитывать, по мнению М. Либики), это не будет гарантировать падение интереса к наращиванию потенциала ведения кибернетических операций, тем более что использование разного рода подставных организаций и сложность идентификации атак весьма способствуют их тайному осуществлению.

Тем не менее в июне 2010 г. в Центре стратегических и международных исследований командующий кибернетическим командованием МО США и директор Агентства национальной безопасности К. Александер выступил с предложением начать переговоры с Россией о подготовке принципиально нового договора, ограничивающего проведение атак в киберпространстве[12]. Надо отметить, что ранее США старались не обсуждать вопросы, связанные с межгосударственным противоборством в информационной сфере, в категориях норм международного права.

США по-прежнему исходят из трёх базовых постулатов, которым должно удовлетворять возможное соглашение и которые в том или ином виде подробно рассматриваются в книге М. Либики[13].

Военное использование киберпространства целесообразно и будет иметь большое значение. Соединённые Штаты не намерены связывать себя какими-либо ограничениями на развёртывание, испытания и использование военных возможностей в этой сфере в целом. В дальнейшем в интересах защиты критически важных американских инфраструктур характеристики кибернетических угроз, по которым возможно подписание международных соглашений, будут детализироваться. Однако вопрос о том, насколько в результате таких соглашений снизится наступательный потенциал США (т.е. целесообразно ли международное обсуждение вообще), должен решаться в ходе всесторонних исследований и моделирования[14].

Соединённые Штаты будут *настаивать на праве осуществлять возмездие (сдерживание)* в случае проведения против них кибернетических атак другими странами. Они твёрдо намерены активно защищать свои инфраструктуры, даже предпринимая упреждающие действия, направленные на срыв кибернетических атак противника.

Поскольку наибольшую проблему в случае проведения кибератаки представляет выявление страны-агрессора, Соединённые Штаты, возможно, *будут заинтересованы в подписании многостороннего соглашения*,

---

[12] *Gorman S.* US Back Talks on Cyber Warfare / Siobhan Gorman // The Wall Street Journal : website. 2010. June 4. URL: http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html.

[13] *Elliott D.* Weighing the Case For a Convention to Limit Cyberwarfare / David Elliott // Arms Control Today. 2009. November. Vol. 39. URL: http://www.armscontrol.org/act/2009_11/Elliott.

[14] *Hamre J.* Cyberwar! : Interview / John Hamre // PBS Frontline. 2003. February 18.

определяющего пропорциональность ответа на кибератаку, исходя из её масштаба, продолжительности и потенциальной угрозы для гражданских объектов. Это, естественно, потребует разработки соответствующего режима верификации.

Таким образом, несмотря на активизацию переговорных усилий в области информационной безопасности, трудно ожидать, что при сложившемся американском подходе российские инициативы о провозглашении информационного пространства зоной, свободной от оружия, найдут поддержку у США и их союзников, уже начавших исследовательские работы по созданию кибернетического оружия. Гораздо более вероятно, что Вашингтон будет всячески пытаться продвигать своё определение понятия "кибернетическая безопасность". И если ему не удастся достичь желаемого на переговорах с Россией, он возложат на неё всю ответственность за отсутствие прогресса, как это уже было при обсуждении европейской конвенции о киберпреступности.

Внимательное прочтение умной и откровенной книги М. Либики лишний раз позволяет в этом убедиться.