

Е.С. ЛАРИНА, В.С. ОВЧИНСКИЙ

## НОВАЯ ВОЕННАЯ СТРАТЕГИЯ США И ПОВЕДЕНЧЕСКИЕ ВОЙНЫ

*Ларина Елена Сергеевна, генеральный директор ООО «Персоналинвест»,  
115093, Москва, Партийный пер., д. 1, к. 58*

*E-mail: elarina@hreshebnik.ru*

*Овчинский Владимир Семенович, д.ю.н., советник Министра внутренних дел РФ,  
119049, Россия, Москва, ул. Житная, д. 16*

*E-mail: vso1955@yandex.ru*

### Аннотация

*Статья посвящена новым нетрадиционным видам вооружений, в ускоренном порядке разрабатываемым в США в соответствии со «Стратегией национальной безопасности 2015» и «Третьей инициативой оборонных инноваций». Проанализированы практические шаги по созданию нового типа поведенческих вооружений, лежащих на стыке использования технологий «больших данных», интеллектуальных вычислений и последних достижений социальной и поведенческой психологии.*

**Ключевые слова:** *поведенческие войны, бихевиористская психология, «большие данные», «Надж», подталкивание, управление массовым поведением.*

В 2015 г. в Соединенных Штатах был принят ряд новых основополагающих документов, определяющих стратегию и тактические действия в сфере национальной безопасности, а точнее сказать, обеспечения глобального доминирования и всемирного диктата, гарантирующего сохранение однополярного мира. Ключевым документом является «Стратегия национальной безопасности США 2015».

В «Стратегии» указано: «Укрепление экономического могущества Америки является основой нашей национальной безопасности и важнейшим источником нашего влияния за рубежом... Мы продолжаем задавать темп развитию науки, технологий и инноваций в глобальной экономике». Дается ответ в «Стратегии» и на вопрос — как обеспечить американскую «исключительность», являющуюся для правящей элиты Америки первостепенной и неоспоримой ценностью: «Успешная стратегия обеспечения безопасности американского народа и продвижения интересов нашей национальной безопасности должна начинаться с одной неоспоримой истины — Америка должна быть лидером»[3].

В рамках стратегии указан и главный враг мирового сообщества. Таким врагом был определен геостратегический субъект, не только препятствующий глобальным планам

США, но и повышающий степень свободы и самостоятельности европейских стран. Еще до начала активной фазы украинского кризиса главным врагом Запада была объявлена Россия. Официально этот тезис был сформулирован в «Стратегии» впервые: «Наши сложные времена наглядно продемонстрировали силу и значимость незаменимого американского лидерства в мире. Мы мобилизовали и возглавили международные усилия по наказанию России и противодействию ее агрессии, по ослаблению, а в конечном счете и по уничтожению ИГИЛ, по искоренению вируса Эболы, по прекращению распространения материалов для изготовления ядерного оружия, по переходу к новому этапу в глобальной борьбе за снижение углеродных выбросов» [3].

Наученные поражениями в Ираке и в Афганистане Соединенные Штаты осуществляют коренную перестройку вооруженных сил, способов и методов их действий. В значительной степени итоги этого пересмотра нашли свое отражение в документе — оперативная Концепция сухопутных сил США «Победа в сложном мире 2020–2040» [3].

В оперативной «Концепции», в документах Пентагона и в выступлениях министра обороны США (с февраля 2015 г.) Эштона Картера указывается, что Соединенные Штаты приняли на вооружение доктрину пяти полей боя и семи сфер противоборств. Полями боя, или, как говорят американцы, доменами являются суша, водная среда, воздух, космос и электромагнитная среда, привычно называемая киберпространством. В качестве семи сфер противоборства выделяются традиционные огневые военные действия, внешнеполитическая борьба, воздействие на внутреннюю политику, финансово-экономические конфликты, информационные войны, поведенческие войны и сфера технологического противоборства.

Несмотря на то, что Соединенные Штаты стараются все в меньшей степени использовать термин «война», заменяя его терминами «жесткое противоборство» или «конфликты», они уверенно ведут мир к перманентному состоянию «мировойны» или «войномира». При этом в новой американской концепции предусматривается, что главная нагрузка ведения традиционных военных действий должна ложиться на союзников, сторонников и поддерживаемые Соединенными Штатами силы. Сами же Соединенные Штаты должны сосредоточиться на скачкообразном развитии и достижении приоритета в новых поколениях ядерных и других сверхразрушительных средств поражения, в качестве последнего аргумента, и главное, максимально использовать нетрадиционные типы вооружений и противоборств. При этом последние по своим разрушительным последствиям смогут не только не уступать, но и превосходить традиционные типы вооружений.

Представляется практически важным (хотя такой подход потребует международно-правовой проработки) относить технологические противоборства, информационные конфликты, поведенческие войны, внутривнутриполитические подрывные акции именно к войнам. Все эти типы жестких противоборств полностью укладываются в определение войны, данное В. Ковалевым, С. Малковым и Г. Малинецким в только что опубликованном докладе «Помни войну»: «Война (жесткое противоборство) — это такой способ ведения конфликта, при котором отсутствуют ограничения на масштабы, инструментарий и методы целенаправленного воздействия на участников конфликта»<sup>1</sup>. По нашему мнению, такое определение является методологически выверенным и операционно эффективным.

Разработка инструментария для войн нового типа стала главной задачей, выдвинутой в прошлом году «Третьей инициативы оборонных инноваций», разработанной на межпартийной основе с участием представителей Администрации, Конгресса, деловых кругов и американских военных. В ходе представления «Третьей оборонной инициативы» бывший министр обороны Ч. Хейгел отметил, что «мы сталкиваемся со стремительным развитием новых технологий, вызовами со стороны различных государств и негосударственных структур; с возникающими сложными, смертельными и часто асимметричными угрозами, начиная от кибератак до деятельности транснациональных преступных сетей. В этой связи министерством обороны США ставится задача действовать на уничтожение и подавление опережающим образом как самой существующей угрозы, так и всех обстоятельств данной угрозы. А главное — резко ограничить возможности субъекта этой угрозы, парализовать или уничтожить его.

<sup>1</sup> URL: <http://spkurdyumov.ru/uploads//2015/05/pomni-voynu.pdf>.

Можно выделить два важнейших обстоятельства, которые обуславливают принятие новой «Инновационной оборонной инициативы». Во-первых, это американское лидерство. Во-вторых, партнерство между государством и бизнесом».

Ч. Хейгел также заявил, что перед лицом происходящих в мире изменений Соединенные Штаты по своим военным и технологическим возможностям, стратегии и готовности к действию должны опережать любого потенциального противника [7].

Выступая в этом году перед руководителями крупнейшим IT- корпораций, венчурных фондов и высокотехнологических компаний, нынешний министр обороны США Эштон Картер выдвинул в качестве первоочередной задачи, которая должна быть решена в ходе реализации «Третьей оборонной инициативы», — создание уникальной системы вооружений, которую ни одна страна в мире не сможет ни скопировать, ни применить в своих целях. Эта система должна использовать уникальные, имеющиеся только в США технологии и монопольно принадлежащие им ресурсы. Частично такая постановка вопроса связана с успехом китайской электронной разведки, которой удалось только за последние три года добыть американских военно-технологических секретов почти на 300 млрд долларов, включая самые современные разработки [6].

Несмотря на многочисленные вопросы со стороны средств массовой информации о характере нового американского оружия на последующей за выступлением пресс-конференции, Э. Картер категорически ушел от ответа, сказав, что сам по себе характер нового типа вооружений не предполагает его широкого обсуждения.

Тем не менее, опираясь на доступные, открытые источники и внимательно анализируя события не только последних месяцев, но и лет, постараемся высказать некоторые предположения относительно того, что же Э. Картер рассматривает как новое стратегическое оружие Соединенных Штатов, способное наряду с ядерными и другими подобными смертоносными арсеналами, сохранить роль Америки, как мирового доминанта.

В любой спецоперации все прямо и косвенно причастные акторы стремятся реализовать собственные цели. Не является исключением и эпопея Э. Сноудена. Вполне очевидно, что он хотел раскрыть глаза американскому и мировому общественному мнению на незаконные методы деятельности АНБ, тотальную слежку и прослушку. В то же время нельзя не отметить, что большая часть разоблачений Сноудена, при всей их сенсационности, не открыла чего-то принципиально нового для экспертов и специалистов в сфере разведки. Практически все, о чем он поведал, было известно до него, хотя и без деталей, подробностей, названий конкретных программ, размеров ассигнованных сумм и т.п. Конечно же, эти детали перевели предположения экспертов из разряда гипотез в сферу конкретных фактов и документированных мнений.

Интересно, однако, посмотреть, каких разделов коснулись разоблачения Э. Сноудена. В основном речь шла о нарушении приватности не только иностранцев, но и граждан США, прослушивании телефонных разговоров не только рядовых американцев, но и глав стран — союзников США, контролем со стороны АНБ за финансовыми транзакциями, осуществляемым по самым разнообразным потокам, программам развития кибервооружений и т.п. Все это произвело чрезвычайно большое впечатление и до сих пор имеет серьезные последствия как для престижа США, так и для межгосударственных отношений. Несомненно, сказалось разоблачения Э. Сноудена и на доходах упомянутых в них компаний.

Тем не менее складывается впечатление, что Агентство Национальной Безопасности использовало казус Э. Сноудена, коль скоро он случился, как стандартную операцию прикрытия в отношении действительно главной, до сих пор тщательно скрываемой задачи, решаемой АНБ и другими государственными структурами США при его содействии. Речь идет о разработке и практическом использовании технологий управления групповым и массовым поведением в других странах мира — как союзниках, так и противниках Соединенных Штатов.

Нетрудно заметить, что в материалах Э. Сноудена вообще не содержится информации на эту тему и, соответственно, может возникнуть предположение, что тезис об управлении групповым поведением сколь угодно большой размерности имеет отношение не к фактическому положению дел, а к конспирологии, причем конспирологии, понимаемой

не в смысле научного, фактологического расследования, а в традиционной трактовке, как измышления незрелого ума и порождения неустойчивой психики.

На сегодняшний день существует достаточно большое количество имеющихся как в открытой печати, так и в специализированных публикациях сведений и данных, подтверждающих гипотезу о переходе определенных групп внутри элиты США к скрытому управлению поведением больших групп населения в самой Америке и за рубежом. Из совокупности разнородных фактов ключевыми, на наш взгляд, являются следующие.

**Первое.** Начать, несомненно, надо с наиболее наглядного, что называется, материализованного свидетельства практической постановки задачи управления поведением. Речь идет о только что отстроенном, оснащенном и выводимом на расчетную мощность циклопическом центре АНБ в штате Юта. Понятно, что для целей шпионажа, радиоэлектронной разведки, криптографии и проч. требуется гигантский объем хранилищ данных. Однако даже для них не нужно хранилище объемом в один йоттабайт, которое расположено в новом дата-центре в штате Юта. Чтобы наглядно понять, о чем идет речь, отметим, что весь ежегодный интернет-трафик, включая собственно Интернет, «интернет вещей» и проч. приближается в настоящее время к одному зеттабайту. Тем самым в Юте имеется хранилище для 15-летнего мирового интернет-трафика. Однако размерность сразу уменьшается в том случае, если не просто хранить трафик, то есть данные всех типов, а обрабатывать их различными способами, для чего представлять данные в виде самых различных классификаций. Иными словами, не для чего иного, как для интеллектуального анализа сверхбольших объемов данных такое хранилище просто не нужно.

**Второе.** В США в отличие от других стран еще в 1994 г. была создана специальная широкополосная сеть для совместного межведомственного использования аппаратных и программных ресурсов суперкомпьютеров. Фактически в Соединенных Штатах, в отличие от других стран, суперкомпьютерная сеть не разделена ведомственными и корпоративными барьерами, а функционирует как единое целое. Более того, в начале нулевых годов американцы договорились с Великобританией, что к этой сети подключаются и британские суперкомпьютеры. Это весьма важно, поскольку, согласно международным оценкам, лидером по эффективности использования суперкомпьютеров в секретных проектах выступает именно Великобритания. Данных по этой сети нигде нет, но различного рода косвенные расчеты позволяют утверждать, что мощность этой сети составит от половины, до двух третей суммарной мощности всех 500 суперкомпьютеров, входящих в настоящее время в мировой рейтинг. Наиболее мощные суперкомпьютеры, входящие в сеть, принадлежат АНБ, Министерству энергетики США, британской разведке и американским университетам, тесно работающим с военно-разведывательным комплексом. С 2014 г. общее руководство сети осуществляет Киберкомандование США (United States Cyber Command – USCYBERCOM).

**Третье.** За последние четыре года Соединенные Штаты истратили несколько сот миллионов долларов на разработку программ интеллектуального анализа не просто больших, а сверхбольших массивов данных. Примечательно следующее обстоятельство. В коммерческом секторе для анализа «больших данных» (Big Data) в основном используются методы математической статистики. В то же время, анализируя гранты таких агентств, как DARPA и IARPA, можно увидеть, что средства затрачивались на разработку таких программ по анализу и прогнозированию на основе «больших данных», которые базируются на принципиально новых разделах математики и теории искусственного интеллекта, типа теории категорий и функторов, на системах распознавания образов, нейронных вычислениях и так называемом глубоком машинном обучении. Все они на порядки превосходят в плане возможности выявления нетривиальных зависимостей и связей, мощности и точности прогнозирования те методы стандартной математической статистики, которые описываются как основной инструмент во всей специализированной литературе по «большим данным».

**Четвертое.** В последние годы в США предпринимаются организационные и законодательные меры по обеспечению потребностей разведсообщества «большими данными». Прежде всего, следует иметь в виду, что само по себе Агентство Национальной Безопасности является обладателем крупнейших массивов «больших данных», получаемых

им в результате своей шпионской деятельности, о которой мир сегодня неплохо осведомлен благодаря разоблачениям Э. Сноудена.

Гораздо менее известна организация FDS (Federal Data Service, в русском переводе она может быть названа «Федеральной службой данных»). Главным ее назначением является концентрация разнообразных данных об американцах, которые собирают практически все федеральные ведомства, министерства, агентства и т.п. Без преувеличения можно сказать, что ни в одной стране мира нет такой подробной базы данных на своих граждан, как в Соединенных Штатах, и находится эта база не в АНБ, а в неприметной организации с указанным выше названием. При этом надо иметь в виду, что в FDS дополнительно стекаются все данные из страховых компаний, банков, пенсионных фондов, авиакомпаний и т.п. под американской юрисдикцией. Соответственно, если те или иные люди застрахованы в американской компании, обслуживаются американскими банками или банками, имеющими корреспондентские счета в американских банках, летали американскими авиалиниями или используют американские кредитные карты, типа Visa, American Express и т.д., то все их данные также попадают в эту организацию, а оттуда — в Центр «больших данных» АНБ.

Э. Сноуден не просто рассказал, а даже показал на слайдах связь с АНБ крупнейших интернет-компаний и телекоммуникационных гигантов. В результате произошел большой скандал. Компании сначала протестовали, затем сообщили, что вносят соответствующие требования в Конгресс США с тем, чтобы прекратить практику использования их данных в интересах АНБ. Однако от публики и даже от большинства экспертов укрылось одно крайне важное обстоятельство. Речь в протестах идет о персональных данных, то есть таких данных, по которым можно идентифицировать пользователя как Ивана Ивановича Иванова, либо Джона Смита Третьего и т.п. В отличие от них, «большие данные» персональными не являются. В принципе они могут относиться к категории «больших данных» — но могут и не относиться. Более того, для технологий «больших данных» сама по себе идентификация конкретного человека не важна и не интересна, потому что связи и закономерности, выявляемые при помощи «больших данных», имеют статистический характер, а не касаются судьбы конкретного индивидуума. Про «большие данные» речь в разоблачениях Э. Сноудена вообще не шла.

Практически все крупнейшие держатели «больших данных» (а ими являются Google, Facebook, Twitter, Amazon, eBay и т.п.) находятся в американской юрисдикции и в случае соответствующих решений, принимаемых в США, обязаны предоставлять все необходимые данные. В отличие от персональных данных, для предоставления обезличенных «больших данных», правительству не нужны даже какие-либо специальные судебные решения. В американском законодательстве четко прописаны обязанности американских компаний с точки зрения национальной обороны.

Важно, что «большие данные» обязаны предоставлять не только американские компании — держатели «больших данных» либо брокеры данных, но и компании, которые котируются на американском биржевом рынке. Последние два обстоятельства нуждаются в некотором пояснении.

В Соединенных Штатах существует целый ряд крупнейших компаний, которые покупают данные по всему миру у других субъектов, как правило, у торговых компаний и перепродают их транснациональным корпорациям для целевого, или как его еще называют таргетированного маркетинга и т.п. В их числе Ascxiom, Experian, Epsilon и т.п. Чтобы представить масштабы накопленных данных, приведем лишь несколько цифр. Только Ascxiom располагает данными на 700 млн человек, что является 10 % всего населения мира. Причем ежедневно число лиц, попадающих в базы данных, возрастает на 0,5–1 млн человек. При этом по подавляющему большинству персон составляются профили, которые включают в себя 150 характеристик [6].

Кроме того, практически все крупные международные интернет-компании котируются на NYSE, либо на Nasdaq. Соответственно, и эти компании при получении запроса также должны под угрозой лишения листинга передавать обезличенные «большие данные» американскому правительству, а иными словами — АНБ. При этом то, что они могут иметь иную юрисдикцию и действовать в далеких от Америки регионах, не является препятствием для выполнения этих обязательств.

Подытоживая, можно сказать, что АНБ сегодня имеет доступ к подавляющему большинству «больших данных», имеющихся в мире. Некоторые высказывают точку зрения, что исключением является Китай, однако другая часть специалистов не без основания полагает, что и китайские «большие данные» в немалой степени оказываются в США через американских и британских брокеров данных.

**Пятое.** В течение последних полутора лет в Соединенных Штатах прошел целый ряд научных конференций, круглых столов и заседаний, инициированных теми или иными «фабриками мысли» (Think Tanks), среди которых выделяется специализирующийся на изучении разнообразных сложных систем Институт Санта-Фе. В этих мероприятиях участвовали ведущие исследователи и разработчики в сфере «больших данных», руководители департаментов поведенческого маркетинга и таргетированной рекламы, специалисты в сфере прогнозирования на основе «больших данных», с одной стороны, и высокопоставленные правительственные чиновники, представители разведывательного сообщества и члены британской и американской правительственных программ «Надж» (Nudge) – с другой. Например, на одной из такого рода конференций с основным докладом «Стратегический потенциал Больших Данных для национальной безопасности» (Strategic Potential of Big Data for National Security) выступила исполнительный директор Агентства передовых исследований в сфере разведки (IARPA, Intelligence Advanced Research Projects Activity) Катарина Марш.

Как правило, в большинстве такого рода мероприятий принимали участие один из ближайших советников Б. Обамы, участник группы по реформе АНБ Касс Санстейн [9], его соавтор по книге «Надж» Ричард Талер [6], а также Алекс Пентланд. Последний был недавно включен журналом «Форбс» в число семи самых влиятельных исследователей в области информационных технологий. Он руководит несколькими лабораториями в знаменитом MIT (Массачусетском технологическом институте), входит в число советников нескольких компаний из списка «Форчун 500», консультирует правительство США.

Чтобы понять, о чем шла речь на этих мероприятиях, достаточно процитировать книгу Алекса Пентланда «Социальная физика»: «Я уверен, что значение «больших данных» состоит в том, что они дают информацию о поведении людей, а не об их убеждениях... Понятие «больших данных» и наука о сетях находятся за гранью обычных подходов к проектированию социальных структур... Адам Смит и Карл Маркс ошибались, или, по меньшей мере, предлагали только половинчатые решения. Почему? Потому что они строили свои теории на основе усредненных понятий рынка и классов. И хотя, безусловно, рассуждение в таких терминах тоже может быть полезным, однако очевидно, что социальные феномены на деле состоят из миллионов мелких транзакций между индивидами. Существуют отдельные примеры межличностных взаимодействий, которые не просто не укладываются в усредненные параметры, а являются причиной социальных всплесков и потрясений, таких как Арабская весна. Придется снизойти до этих мельчайших примеров, этих микропримеров, потому что они позволяют понять социальное устройство вне усредненных показателей. Мы вступаем в новую эру социальной физики, где решающий исход будет зависеть от самых мелких деталей, от таких мелочей, как ты да я... Сам факт того, что мы теперь сможем отслеживать динамику социальных взаимодействий и их происхождение, что мы больше не будем ограничены усредненными показателями, такими как рыночные индексы, вызывает во мне трепет. Мы будем способны предсказывать поведение рынков и возникновение революций и управлять ими» [8].

На этих конференциях родился пока еще не получивший широкого признания термин «hidden power», или «невидимая сила».

Вполне очевидно, что представленные факты носят комплементарный, то есть дополняющий друг друга характер и показывают целостную картину завершающего этапа создания технологической системы управления групповым и массовым поведением любой размерности в иностранных государствах для реализации интересов наднациональной финансово-корпоратократической элиты.

Итогом такого управления должно стать превращение субъектов мировой политики, экономики и т.п. в объекты, находящиеся под внешним, не воспринимаемым, руководящим воздействием. Для того, чтобы этого не случилось, необходимо в крайне сжатые сроки

осуществить комплекс весьма интеллектуалоемких, высокотехнологичных мер, подкрепленных целым рядом обеспечивающих мероприятий, требующих затрат ресурсов и принятия новых юридических актов на государственном уровне.

Отдельная тема – это поведенческие войны. В настоящее время практически невозможно найти западных публикаций, посвященных данной теме. В значительной степени это связано с ее чрезвычайной деликатностью, в том числе, для западного общественного мнения. Кроме того, возможности ведения полноценных поведенческих войн появились лишь недавно в связи с накоплением огромных массивов объективной информации о человеческом поведении, в том числе поведении социальных и иных групп сколь угодно большой размерности. Эти сведения в основном содержатся в интернете, который по факту является огромным поведенческим архивом.

Возможности поведенческих войн связаны с инструментарием, разрабатываемым на стыке когнитивных вычислений, «больших данных» и междисциплинарного комплекса поведенческих наук. Давно и хорошо известно, и особый вклад внесли в это российские психологи, что человеческое поведение в значительной мере зависит не только от наших представлений, ценностей, убеждений, а в немалых своих компонентах базируется на стереотипах, привычках, поведенческих паттернах, а также складывается под воздействием формальных и неформальных институтов.

Доказано, что человек по своей психофизиологии склонен, как и любое живое существо, к решению задач с меньшей, по возможности, затратой энергии и других ресурсов. Поэтому, как неопровержимо установили исследователи, значительная часть нашего поведения осуществляется в своего рода полуавтоматическом режиме, на основе привычек и стереотипов. Это касается не только элементарных поведенческих функций и стандартных жизненных ситуаций. Наши привычки, поведенческие паттерны, культурные стереотипы и т.п. оказывают серьезное воздействие даже в сложных ситуациях выбора, казалось бы, требующих глубоких размышлений и мобилизации ресурсов сознания.

Хорошо известно, что деятельность человека контролируется не только работой его сознания. Многие важнейшие функции человек делает, что называется, бессознательно. На протяжении практически 50 лет этот тезис получил множество подтверждений на основе огромного массива впечатляющих экспериментов, значительную роль в проведении которых сыграли советские психологи. Сегодня на основе, в том числе, и их исследований, с привлечением огромных массивов данных о реальном поведении людей в различных ситуациях, их привычках, склонностях и реакциях и разрабатывается арсенал принципиально нового вида войн – поведенческих войн.

В их сердцеvine лежит манипулирование вложенными в нас социумом, а также собственной биографией и культурной средой, алгоритмами поведения, привычками, стереотипами деятельности и т.п. Грубо говоря, инструментарий поведенческих войн состоит в том, чтобы отделить привычку от сложившегося вида деятельности, сформировавшей ее ситуации, и использовать поведенческие паттерны для достижения иных целей.

Поведенческое оружие – это оружие завтрашнего дня. Именно под него заточен только что пущенный в эксплуатацию и уже упоминавшийся выше супергигантский по своей информационной емкости центр АНБ в штате Юта, который аккумулирует массивы поведенческой информации, охватывающие все страны мира и все континенты. Именно на этот новый вид вооружений возлагаются частью американских элит наибольшие надежды в жестких противоборствах ближайшего будущего. Тема поведенческих войн не только не афишируется, но, напротив, в наибольшей мере табуирована и засекречена в мировом информационном пространстве. Более того, согласно распространенной точке зрения, ведущие американские средства массовой информации, наиболее популярные блоггеры и т.п. имеют негласную рекомендацию: при появлении каких-либо материалов на тему поведенческих войн дискредитировать их любыми доступными средствами, начиная от обвинений в конспирологии и заканчивая доказательством о якобы технологической невозможности ведения поведенческих войн.

В заключение скажем о соотношении информационных и поведенческих войн. В значительной степени это вопрос терминологии. Более того, в Великобритании, где впервые появился термин «бехивеористские» или поведенческие войны, их связывали

с использованием конкретной школы психологии, а именно школы бихевиоризма Б. Скиннера [4]. Что касается американских исследователей, особенно школы «Надж», то они в значительной мере опирались на работы Д. Канемана и А. Тверского, в которых традиционно использовался термин «бихевиористская», то есть поведенческая экономика [9].

Представляется, однако, что различие между поведенческими и информационными войнами носит не терминологический, а принципиальный, в том числе инструментальный и конструктивный, характер. И аргументом в пользу этого может послужить то обстоятельство, что человеческая деятельность, а соответственно, и поведение, выходят за пределы чистой обработки информации, что было убедительно показано, в частности, выдающимся советским психологом Э.В. Ильенковым и другими представителями отечественной психологической науки [2; 5], для чего ими был в свое время проведен беспрецедентный эксперимент по обучению слепоглухонемых детей. Информация является лишь одним из составных компонентов поведения, которая обязательно предполагает различного рода инструментальную деятельность, психофизиологические реакции и иные чисто физические процессы. В поведенческих войнах используется инструментарий не только информационных войн самого различного типа, в том числе базирующийся на семиотических системах, но и различного рода физические, ориентационные и иные технологии.

## THE NEW US MILITARY STRATEGY AND BEHAVIORAL WARS

*Elena Larina, General Manager «Personalinvest», 115093,  
Moscow, Partijny per., d. 1, k. 58 E-mail: elarina@hreshebnik.ru*

*Vladimir Ovchinsky, Doctor of Law, Adviser to the Minister of Internal Affairs of the Russian  
Federation, 119049, Russia, Moscow, ul. Zhitnyaya, d. 16  
E-mail: vso1955@yandex.ru*

### Summary

*The Article is devoted to new nonconventional types of weapon, in the accelerated order of the defensive innovations developed in the USA according to Strategy of national security the 2015 and Third initiative defense innovation. Practical steps on creation of new type of behavioral weapon, laying on a joint of use of technologies of Big Data, intellectual calculations and last achievements of social and behavioral psychology are analyzed.*

**Key words:** *behavioral wars, behavioristic psychology, Big Data, Nudge, management of mass behavior.*

## ЛИТЕРАТУРА / REFERENCES

1. Канеман Д., Словик П., Тверский А. Принятие решений в неопределенности: правила и предубеждения. — М., 2005.
2. Мареев С.Н., Ильенков Э.В. Жить философией. — СПб., 2015.
3. Мировойна: все против всех. Новейшие концепции англо-саксонской военной мысли / Под ред. Е. Лариной и В. Овчинского. — М., 2015.
4. Слейтер Л. Открыть ящик Скиннера, АСТ. — М.: 2007.
5. Ильенков Э.В. Сборник статей / Под ред. В.И. Толстых. — М.: РОССПЭН, 2009.
6. Goodman M. Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It. — N.Y., 2015.
7. Hagel Ch. A Keynote Speech delivered at Reagan Presidential Library, Simi Valley, CA, November 15, 2014. URL: <http://www.defense.gov/News/Speeches/Speech-View/Article/606635>
8. Pentland A. Social Physics: How Good Ideas Spread-The Lessons from a New Science, Penguin Press; 2014.
9. Sunstein C.R. Why Nudge?: The Politics of Libertarian Paternalism (The Storrs Lectures Series), Yale University Press; 2015.
10. Thaler R.H. Misbehaving: The Making of Behavioral Economics, W. W. Norton & Company; 2015.
11. Thaler R.H., Sunstein C.R. Nudge: Improving Decisions About Health, Wealth, and Happiness, Penguin Books; 2009.