АЛЕКСАНДР СМИРНОВ

Информационно- психологическая война

Об одном средстве международного
информационного противоборства

Невидимая война: вступительные замечания

Значительное возрастание значимости информационной сферы жизни общества во второй половине XX — начале XXI века и увеличение потенциала средств информационного воздействия на общество обусловили их включение в арсенал инструментов межгосударственного противоборства. Информационные средства и методы борьбы не являются изобретением XX столетия — история их развития насчитывает не одно тысячелетие. Еще выдающийся китайский мыслитель Сунь Цзы (конец VI — начало V века до н. э.), автор одного из наиболее известных ныне древнекитайских трактатов по военному искусству, описывал многочисленные способы морально-психологического воздействия на противника¹.

Однако именно XX век является тем историческим периодом, в котором началась «информационная революция», продолжающаяся до настоящего времени. Учитывая значимость

этого явления, сегодня ощущается острая необходимость четкого определения таких важных понятий, как «информационное противоборство», «информационная война», «психологическая война», «кибервойна» и др. Этой задаче и посвящена настоящая статья, в центре внимания автора которой находится феномен информационно-психологической войны как направления информационного противоборства.

Наиболее общим и широким понятием является *информационное противоборство* (далее — ИП). Так, И. Н. Панарин определяет его как форму борьбы сторон с применением специальных (политических, экономических, дипломатических, военных и иных) методов, способов и средств воздействия на информационную сферу противостоящей стороны, а также в целях самозащиты². Полагаем, однако, что применительно к этому определению требуют уточнения три основных момента, определяющие содержание рассмат-

¹ См. **И. Н. Конрад**. Сунь-Цзы. Трактат о военном искусстве. М., 1950.

² См. **И. Н. Панарин**. Информационная война и геополитика. М., 2006. С. 172. Схожее определение см. в книге: **Д. Н. Шакин и др.** Информационная безопасность. М., 2009. С. 136.

СМИРНОВ Александр Александрович — ведущий научный сотрудник ФГКУ «ВНИИ МВД России», доцент, кандидат юридических наук.

Ключевые слова: информационное противоборство, информационное оружие, информационно-психологическая война, подрывная деятельность.

риваемого понятия: вопрос о субъекте ИП; вопрос об объекте ИП; вопрос о средствах и методах ИП.

В первом случае можно выделить в качестве субъектов ИП исключительно государства и их учреждения либо расширить круг таковых за счет международных и неправительственных организаций, незаконных вооруженных формирований и террористических (экстремистские) структур, а также ТНК, включая медиа-корпорации³. Иногда, однако, в круг субъектов ИП, помимо международных акторов, включаются также организации и лица, действующие внутри страны (коммерческие компании, национальные НКО, СМИ и т. д.)⁴.

Характер объекта ИП у большинства исследователей сомнения не вызывает: в качестве такового, как правило, называется информационная сфера либо ее отдельные элементы — информация, информационные системы и информационная инфраструктура. Такой подход разделяется нами при условии включения самого человека и социальных групп в состав информационной сферы как разновидностей информационных систем. Наконец, говоря о средствах и методах ведения ИП, мы полагаем целесообразным рассматривать в качестве таковых лишь виды борьбы, в рамках которых применяются информационные средства и методы воздействия.

Еще одним базовым понятием в изучаемой области является *информационная война* (далее — ИВ) —

³ См., например: **А. В. Манойло**. Объекты и субъекты информационного противоборства. — «ПСИ-ФАКТОР» (<http://psyfactor.org/lib/psywar24.htm>); **Д. Б. Фролов**. Информационное противоборство в сфере геополитических отношений. Автореф. дис. ... докт. полит. наук. М., 2006. С. 9 и др.

⁴ См. об этом, например: **А. Е. Соловьева**. Информационное противоборство в сети Интернет: политологический анализ. Автореф. дис. ... канд. полит. наук. Пятигорск, 2011.

термин, введенный в США в 1976 году, но привлечший внимание экспертов после войны в Персидском заливе в 1991-м (операция «Буря в пустыне») ⁵. В американских официальных документах и научной литературе для обозначения ИВ используется единый термин «Information Warfare» (далее — IW), который можно перевести и как «информационная война», и как «информационное противоборство» ⁶. Учитывая милитаристское происхождение данного понятия, его американские дефиниции были ориентированы под военные цели (ведение войны). При этом акцент делается на необходимость воздействия на противника еще в угрожаемый период, то есть до начала активных боевых действий ⁷. В дальнейшем, однако, от термина ИВ (IW) отказались, заменив его понятием *информационные операции* (Information Operations, IO). При этом, помимо IW и IO как сферы действия американских вооруженных сил, в США выделяются и иные направления информационного противоборства, в которых задействованы невоенные структуры (Государственный департамент, ЦРУ и др.). Для их обозначения используются иные термины — такие, как *публичная дипломатия* (*public diplomacy*), *стра-*

⁵ См. «Информационные, специальные, воздушно-десантные и аэромобильные операции армий ведущих зарубежных государств. Информационно-аналитический сборник». А. Н. Сидорин, И. А. Рябченко, В. П. Герасимов и др. М., 2001. С. 7–8. См. также: **К. Борিশполец**. Информационное противоборство и его особенности. 31.09.2009. — www.mgimo.ru/news/experts/document138528.phtml

⁶ См. «Сводный глоссарий Совета Россия—НАТО по сотрудничеству». М.; Брюссель, 2011. С. 167, 488–489.

⁷ См.: «Информационные, специальные, воздушно-десантные и аэромобильные операции армий ведущих зарубежных государств». С. 7; **А. В. Бедрицкий**. Реализация концепции информационной войны военно-политическим руководством США на современном этапе: Автореф. ... канд. полит. наук. М., 2007. С. 24.

тегическая коммуникация (strategic communication), тайные операции (covert operations) и т. п. Это важно учитывать при использовании термина «ИВ» и его американских толкований.

В нашей стране одним из наиболее кратких и удачных определений ИВ представляется вариант, предложенный С. Н. Гриняевым, согласно которому под ИВ понимается «широкомасштабная информационная борьба с применением средств информационного воздействия на противника в интересах достижения целей воздействующей стороны»⁸. Большая детализация присуща определению ИВ, содержащемуся в двух международных актах: «Информационная война — противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массивированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны»⁹.

⁸ С. Н. Гриняев. Поле битвы — киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. Минск, 2004. С. 97. Близкую точку зрения см. В. Ф. Прокофьев. К проблеме формирования основных понятий в области информационной безопасности. — «Военная безопасность Российской Федерации в XXI веке. Сборник научных статей». М., 2005. С. 237.

⁹ См. «Соглашение между правительствами государств—членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года». — «Бюллетень международных договоров». 2012. № 1. С. 13—21. Кроме того см. «Конвенция об обеспечении международной информационной безопасности (концепция)». Совет безопасности РФ. — <http://www.scrf.gov.ru/documents/6/112.html>

Большинство отечественных исследователей выделяет два основных направления (или вида) ИВ (ИП): *информационно-техническое*, объектами воздействия которого являются информационно-технические системы (системы связи и управления, компьютерные и телекоммуникационные системы, радиоэлектронные средства и т. д.), и *информационно-психологическое*, для которого в качестве таковых выступают информационно-психологические объекты (психика человека и общественное сознание)¹⁰. В связи с этим едва ли можно согласиться в Е. Лариной и В. Овчинским, которые определяют ИВ как «контентные войны, имеющие своей целью изменение массового, группового и индивидуального сознания»¹¹, то есть фактически сводят их к информационно-психологическим войнам.

Более детальный перечень направлений ИВ приведен в официальных документах США. В них выделяются пять основных видов информационных операций:

- радиоэлектронная борьба (Electronic Warfare, EW);
- психологические операции (Psychological Operations, PSYOP);
- сетевые операции (Computer Network Operations, CNO);
- мероприятия по оперативной маскировке (Military Deceptions, MILDEC);

¹⁰ См.: С. Н. Гриняев. Поле битвы — киберпространство. С. 97—100; В. Ф. Прокофьев. К проблеме формирования основных понятий в области информационной безопасности. С. 237; И. Н. Панагин. Информационная война и геополитика. С. 173; К. Ю. Будылин. Информационное противоборство в военной сфере (политологический анализ): Автореф. дис. ...канд. полит. наук. М., 2009. С. 11; «Война и мир в терминах и определениях». М., 2004. С. 75.

¹¹ Е. Ларина, В. Овчинский. Цифровая война. — «Завтра». 07.11.2013.

— мероприятия по обеспечению собственной безопасности сил и средств (Operations Security, OPSEC)¹².

Как видно, и здесь в определенной степени прослеживается выделение психологических и технических направлений ИП.

Для обозначения инструментария ведения ИВ используется термин *информационное оружие* (Information Weapon). Проект Конвенции об обеспечении международной информационной безопасности определяет информационное оружие (далее — ИОр) как «информационные технологии, средства и методы, предназначенные для ведения информационной войны». В. Ф. Прокофьев приводит схожую дефиницию, конкретизирующую объекты воздействия: «совокупность способов и средств воздействия на технику и людей с целью решения задач воздействующей стороны»¹³. ИОр также подразделяется на два вида: информационно-техническое и информационно-психологическое.

Интересно отметить, что, хотя ИПсВ в настоящее время рассматривается как вид ИВ, само понятие «психологическая война», равно как и его концепция появились намного раньше — в период между концом 1920-х и концом 1940-х годов. В 1949 году был принят первый полевой устав Армии США FM-33-5 «Психологическая война в боевых операциях» (Psychological Warfare in Combat Operations). Еще ранее, в 1942-м, в Америке было учреждено Управление военной информации (United States Office of War Information), а в 1959-м — Управление командования психологической войной (Office of the Chief of Psychological

Warfare)¹⁴. Для сравнения: в СССР термин «ИПсВ» появился намного позднее — лишь во второй половине XX века¹⁵.

П. Лайнбарджер, одним из первых использовавший термин ПсВ, рассматривает его содержание в широком и узком смыслах: в первом — как «использование основ психологии в военном деле», во втором — как «использование пропаганды в вооруженной борьбе с одновременным ведением таких боевых действий, которые дополняют пропаганду»¹⁶. В военном Наставлении 33-5 по ведению психологической войны 1955 года (FM 33-5 Psychological Warfare Operations, 1955) ПсВ определялась как «планомерное ведение пропаганды, главная цель которой заключается в том, чтобы влиять на взгляды, настроения, ориентацию и поведение войск и населения противника, населения нейтральных и союзных стран, с тем чтобы содействовать осуществлению государственных задач»¹⁷. Таким образом, ПсВ, по существу, выводилась за рамки вооруженной борьбы (сферы действия вооруженных сил) и рассматривалась гораздо шире, что вполне адекватно сути явления.

¹⁴ См. **В. М. Bemis**. Cooking up psychological operations: the ingredients of successful PSYOP. Thesis. Naval Postgraduate School. Monterey (California), 2011. P. 1. (www.dtic.mil/dtic/tr/fulltext/u2/a547748.pdf).

¹⁵ См.: **Г. Зазворка**. Психологическая война НАТО. М., 1963; **А. Ф. Бобиков**. Психологическая война империалистических государств против стран социализма и пути борьбы с подрывной пропагандой противника: Дис. ...канд. пед. наук. М., 1966. См. также: **Д. А. Волкогонов**. Психологическая война: Подрывные действия империализма в области общественного сознания. М., 1984.

¹⁶ **П. Лайнбарджер**. Психологическая война. Пер. с англ. М., 1962. С. 46.

¹⁷ *Цит. по:* **А. И. Ракитов**. Предисловие к русскому изданию. — **П. Лайнбарджер**. Психологическая война. С. 5—6.

¹² См. «Joint Publication 3-13 Information Operations 2006». P. 9.

¹³ **В. Ф. Прокофьев**. К проблеме формирования основных понятий в области информационной безопасности. С. 237.

Информационно-психологическая война

С учетом сказанного обратимся непосредственно к определению феномена *информационно-психологической войны*. В отечественной и зарубежной научной литературе это понятие чаще употребляют без слова «информационно» и обозначают просто как «психологическая война» (Psychological Warfare, PSYWAR). Термины «информационно-психологическая война» (далее — ИПсВ) и «психологическая война» (далее — ПсВ) будут использоваться нами в качестве тождественных.

В армейских наставлениях по ПсВ, принятых в последующие годы, Министерство обороны США отказалось от термина «ПсВ» (PSYWAR) и заменило его на «психологические операции» (Psychological Operations, PSYOP; далее — ПсО). Последние определяются ныне как «спланированные операции по передаче определенной информации и сигналов иностранной аудитории с целью оказания влияния на их эмоции, мотивы, целеполагание и в конечном итоге на поведение иностранных правительств, организаций, социальных групп или индивидов». Целью ПсО является «формирование или усиление установок и поведения иностранной аудитории в соответствии с целями воздействующей стороны». Очевидно, что такие операции можно проводить по мере необходимости, не задаваясь вопросом о наличии или отсутствия «состояния войны» с противником, пусть и психологической.

В конце первого десятилетия XXI века в США было принято решение отказаться от устоявшегося и получившего широкое хождение в военных и научных кругах понятия «ПсО» (PSYOP) и заменить его новой категорией «Military Information

Support Operations» (MISO), которую можно перевести как «операции информационной поддержки военных действий»¹⁸. В 2010 году было принято новое Наставление с таким названием (Joint Publication 3-13.2. Military Information Support Operations, 2010), и соответствующие изменения были внесены в базовый официальный словарь военных терминов¹⁹. Однако обращение к содержанию нового Наставления показывает, что содержание MISO осталось таким же, как и у PSYOP. То есть имеет место «ребрендинг» без внесения концептуальных изменений в саму деятельность.

В отечественной литературе ИПсВ с начала 1970-х годов трактовалось как «комплексная форма подрывной деятельности империалистического государства, включающая разведывательные, пропагандистские, дипломатические, военные мероприятия, направленные на подрыв политической власти, морально-психологического состояния населения и вооруженных сил их политических противников, изменение их внутренней и внешней политики»²⁰; подчеркивалось, что ПсВ ведется как в мирное, так и в военное время. Поддерживая такой подход к трактовке ПсВ, вместе с тем полагаем, что он имеет один важный недостаток — неоправданное расширение ее содержания за счет отнесения к средствам ПсВ не только пропагандистских, но и иных мероприятий подрывного характера (дипломати-

¹⁸ И. Левкин переводит термин как «операции по информационному обеспечению действий войск» (см. **И. Левкин**. Операции без выстрелов и взрывов. — «Военно-промышленный курьер». 2012. № 20 (447).

¹⁹ См. «Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1–02. 08 November 2010, as amended through 15 August 2013». P. 184. — www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

²⁰ «Психологическая война». — «Контрразведывательный словарь». Отв. ред. В. Ф. Никитченко. М., 1972. С. 239.

ческих, военных и т. п.). В этом смысле более обоснованной представляется позиция авторов российской Доктрины информационной безопасности Российской Федерации, которые обозначили данную угрозу информационной безопасности как «диверсионно-подрывную деятельность специальных служб иностранных государств, осуществляемую методами информационно-психологического воздействия».

Информационно-психологическую войну можно определить как масштабное применение средств и методов информационно-психологического воздействия в отношении населения страны, отдельных социальных групп или индивидов и защиту от аналогичных действий в свой адрес, осуществляемое государством или иным актором международной политики для обеспечения реализации своих интересов.

Пониманию характера ПсВ в советский период был присущ ярко выраженный идеологический подход²¹. Однако если абстрагироваться от чрезмерной идеологизации, то окажется, что суть тогдашних трактовок понятия вполне соответствует и современным отечественным концепциям. Так, например, В. Ф. Прокофьев определяет ИПсВ как «широкомасштабное применение способов

и средств информационного воздействия на психику личного состава войск и населения в интересах достижения воздействующей стороной политических, дипломатических, военных, экономических и других целей»²². Очевидно, что ИПсВ выходит далеко за рамки психологического обеспечения военных операций и рассматривается как средство обеспечения национальных интересов в целом. Важным дополнением к приведенному определению является указание на то, что ИПсВ включает защиту от указанных действий со стороны врага²³.

Итак, ИПсВ можно определить как масштабное применение средств и методов информационно-психологического воздействия в отношении населения страны, отдельных социальных групп или индивидов и защиту от аналогичных действий в свой адрес, осуществляемое государством или иным актором международной политики для обеспечения реализации своих интересов.

При этом в качестве основных целей ИПсВ выступают следующие:

— обеспечение принятия решений и совершения действий объектами воздействия, отвечающих интересам субъекта ведения ИПсВ;

²² В. Ф. Прокофьев. К проблеме формирования основных понятий в области информационной безопасности. С. 237.

²³ «Война психологическая». — «Война и мир в терминах и определениях». Под общ. ред. Д. Рогозина. М., 2004. С. 76.

²¹ См. Д. А. Волкогонов. Психологическая война. С. 6.

— подрыв легитимности политической власти, международного авторитета атакуемой страны;

— дестабилизация ситуации в стране, провоцирование политических протестов, социальных конфликтов;

— провоцирование возникновения и развития иных негативных социальных явлений в стране, способствующих снижению ее жизнестойкости;

— подрыв морально-психологического состояния населения страны;

— подрыв обороноспособности государства, включая боеспособность вооруженных сил;

— содействие самоуничтожению объекта воздействия или причинения им себе вреда;

— изменение социально-культурной идентичности населения страны, национальных ценностей и устоев.

Можно также выделить и промежуточные цели, состоящие во влиянии на эмоции, мотивы, целеполагание и иные индивидуальные и коллективные психологические структуры (процессы) и изменении их в нужном направлении, на чем делается акцент в американских официальных документах и трудах некоторых российских исследователей²⁴.

В качестве основных *объектов*, подвергающихся информационно-психологическому воздействию в ходе ведения ИПсВ, выступают: политическая элита; население страны в целом; отдельные социальные группы (национальные, религиозные, профессиональные и т. д.); отдельные лица (глава государства, начальник генерального штаба вооруженных сил, политический оппозиционер, военнослужащий на объекте СПРН²⁵

и т. п.). Не случайно, в официальных актах США и НАТО в качестве направления противоборства выделяется «*дезорганизация системы управления противника*» («*command and control warfare*»), включающая комплекс мероприятий с использованием всех военных возможностей с целью предотвращения поступления информации в органы командования и управления противника, оказания на них воздействия, их подрыва или уничтожения, наряду с защитой своих органов командования и управления от подобных действий. Среди указанных «военных возможностей» названы разные виды ИВ, включая психологические операции²⁶.

Субъекты ИПсВ

В отличие от традиционных вооруженных конфликтов, где круг участников (комбатантов) в большинстве случаев четко очерчен и включает в себя специализированные военные государственные структуры (вооруженные силы, иные военизированные формирования), хотя допускает вовлечение и иных акторов (например, партизанских отрядов), для ИПсВ свойственно активное участие негосударственных структур в проведении ПсО. При этом в последние годы все большую роль в рамках ИПсВ стали играть новые «воины» — *блогеры* и *хакеры*, а также *неструктурированные сетевые сообщества*.

В качестве *блогеров* выступают частные лица, являющиеся продвинутыми пользователями Интернета и ведущими собственные блоги, ко-

²⁴ См. А. В. Манойло, А. И. Петренко, Д. Б. Фролов. Государственная информационная политика в условиях информационно-психологической войны. М., 2009. С. 274.

²⁵ Система предупреждения о ракетном нападении.

²⁶ См. «Joint Publication 3-13. Joint Doctrine for Information Operations 1998». P. GL-4. — www.c4i.org/jp3_13.pdf; «Joint Publication 3-13.1. Joint Doctrine for Command and Control Warfare (C2W) 1996». — www.iwar.org.uk/rma/resources/c4i/jp3_13_1.pdf; «Дезорганизация системы управления противника (command and control warfare, C2W)». — «Сводный глоссарий Совета Россия—НАТО по сотрудничеству». С. 448.

торые добровольно или по команде вовлекаются в процесс ведения ИПсВ. Их основная роль в ИПсВ сводится к размещению в своих блогах, на страницах социальных сетей, собственных и сторонних сайтах различной информации: видеозаписей, фотографий, статей, комментариев и прочего контента — с целью причинения вреда атакуемому объекту либо противодействия деструктивному психологическому воздействию с его стороны. *Хакеры* — это лица, использующие интернет-технологии для причинения ущерба компьютерным сетям и их пользователям. Они участвуют в ИПсВ посредством компьютерных атак на информационные ресурсы «вражеской стороны» с целью нарушения их работы и (или) размещения пропагандистской информации на них после взлома. *Неструктурированные сетевые сообщества* (далее — НСС) объединяют обе названные категории лиц под определенным общим брендом и идеей. Несмотря на отсутствие официального статуса и четкой структуры, такие сообщества имеют общую концепцию своей деятельности и занимаются ею на постоянной основе. Наиболее известными такими сообществами в мире являются «Anonimus», «WikiLeaks», «LulzSec».

Использование возможностей коммуникаций в социальных сетях в целях политической борьбы получило специальное название — «*хактивизм*» (*Hactivism*). Оно возникло из соединения двух слов «hack» и «activism» и обозначает новую форму социального протеста, являющуюся синтезом социальной активности, преследующей цель протеста против чего-либо, и хакерства²⁷. Несмотря

²⁷ См. **Т. Сайтарлы**. «Hack» + «Activism» = хактивизм. — «Центр исследования компьютерной преступности». 20.04.2004 (www.crime-research.ru/news/20.04.2004/92/).

на то, что хактивизм больше проявляет себя во внутривнутриполитической борьбе за права человека и свободу Интернета, его субъекты активно заявили о себе и в международной сфере, включая конфликты международного характера.

В частности, причиной, побудившей руководство НАТО заняться выработкой стратегии кибербезопасности, стали массированные кибератаки на правительственные сайты Эстонии весной 2007 года в ответ на решение эстонских властей о переносе памятника Воину-Освободителю («Бронзового солдата»). Целями атак хакеров стали серверы парламента, президента, госканцелярии, МИД, минобороны, крупнейших банков и газет. На сайте правящей Партии реформ хакеры вывесили фальшивое извинение премьера А. Ансипа за перенос «Бронзового солдата»²⁸. В компьютерных нападениях представители эстонских властей обвинили российскую сторону, хотя позже выяснилось, что атаки происходили с территорий 76 стран²⁹. Коллективной реакцией стран НАТО на эти события стали учреждение в Таллине Центра коллективной киберобороны НАТО (NATO Cooperative Cyber Defence Centre of Excellence) и выработка знаменитого Таллинского руководства о применимости международного права к кибервойнам³⁰.

²⁸ См. **Е. Родина, В. Соловьев**. Серверно-атлантический альянс. Эстония поднимает НАТО на борьбу с российским интернет-терроризмом. — «Коммерсантъ». 17.05.2007; **А. Д. Реевский**. Кибертерроризм — виртуальный инструмент реальной войны. — «Бюллетень Центра европейской безопасности». 2011. Вып. 23 (39). С. 12–15.

²⁹ См. «Эксперты по безопасности: Кибертерроризм — это миф, и его значение переоценивают». — «SecurityLab.ru». 18.04.2008 (www.securitylab.ru/news/351684.php).

³⁰ The Tallinn Manual. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2007. — www.ccdcoe.org/249.html

Что же касается деятельности отдельных блогеров, то наиболее ярко они проявили себя в известных событиях «Арабской весны» — серии революционных выступлений в странах Ближнего Востока и Северной Африки в 2011—2012 годах³¹. В частности, большую известность получил египетский блогер Ваэль Гоним, который создал в социальной сети «Facebook» аккаунт «Кулена Халед Саид» («Каждый из нас Халед Саид») в память об убитом полицией Египта политическом активисте, ставший одним из ключевых ресурсов сбора и распространения информации, дискредитирующей режим Хосни Мубарака, и организации политических протестных акций на улицах египетских городов, закончившихся в итоге революцией и падением режима египетского лидера³².

Показательны также примеры «сетевых медиабоев на Ближнем Востоке»³³: выясняется, что военные операции Израиля в секторе Газа сопровождаются активной информационной поддержкой, которую осуществляют государственные структуры и привлекаемые ими волонтерские социальные сети. Для подготовки сетевых активистов открыт специальный Междисциплинарный центр в курортном пригороде Тель-Авива Герцлия (Interdisciplinary Center at Herzliya,

IDC), имеющий прочные связи с израильской разведкой. Противостоящая Израилю палестинская группа ХАМАС также активно задействует IT-специалистов для сетевой войны. Их подготовка осуществляется в Исламском университете Газы, известном своими связями с ХАМАС.

Приведенные примеры не только убедительно доказывают тезис о возрастающей роли сетевых активистов и их объединений в ИПсВ новейшего времени, но и демонстрируют возможности использования ими новейших инструментов сетевого противоборства поколения Web 2.0.

С учетом изложенного, полагаем возможным представить авторский вариант видения институциональной системы ведения ИПсВ, которая включает в себя следующие виды *субъектов ИПсВ*:

1. *Национальные войсковые подразделения психологических операций* (4-я группа психологических операций армии США, 950 батальон связи бундесвера, 15-я группа психологических операций вооруженных сил Великобритании и т. п.) — их основной задачей является ведение пропаганды во время вооруженного конфликта или в угрожаемый период в отношении военного контингента государства-противника и проживающего на его территории населения в целях их деморализации, побуждения к отказу от сопротивления, сдаче в плен и т. п.

2. *Государственные внешнеполитические органы* (Государственный департамент США, американский Совет управляющих по вопросам вещания, и т. п.) — их функциональная роль сводится к оказанию «мягкого» информационного воздействия с целью обеспечения пропагандистской поддержки действий государства международным сообществом (включая проводимые военные опе-

³¹ См.: «Политическое цунами. Аналитика событий в Северной Африке и на Ближнем Востоке». Под ред. С. Кургияна. М., 2011; **А. И. Чернобай**. Роль социальных сетей в мобилизации протестных настроений на Ближнем Востоке и в Северной Африке в январе-марте 2011 года. — «Идеологические аспекты военной безопасности (научно-практическое приложение к журналу «Армия» Министерства обороны Республики Беларусь)». 2011. № 1. С. 40—47.

³² См. **В. Гоним**. Революция 2.0: Документальный роман. Пер. с англ. Т. Даниловой. СПб., 2012.

³³ См. **В. И. Газетов, М. Н. Ветров**. Сетевые бои на Ближнем Востоке. — «Независимое военное обозрение». 2013. № 27.

рации) развития гуманитарного сотрудничества, а также дискредитации потенциального или реального противника.

3. *Специальные службы государства* (ЦРУ США, Федеральная разведывательная служба Германии, Пакистанская межведомственная разведка и т. п.) — осуществляют проведение тайных подрывных операций в государстве, поиск, вербовку и использование «агентов влияния» среди политического и военного руководства страны, политической оппозиции и бизнес-элиты, осуществляют тайные лонгитюдные ПсО, а также противодействуют ведению ИПсВ противником методами контрразведывательного характера.

4. *Органы военной и политической пропаганды международных организаций* (Объединенный информационно-аналитический центр НАТО, Объединенный штаб ОДКБ и т. п.) — организуют ведение политической пропаганды в мирное время и военной — в угрожаемый период, а с началом военного конфликта — в дополнение к усилиям национальных государств, входящих в состав данной организации; а также координируют их действия между собой.

5. *Международные неправительственные организации* (американский Фонд поддержки демократии, германский Фонд Фридриха Наумана и т. п.) — их функциональная роль весьма разнообразна, включая оказание информационного «давления» на политическое и военное руководство страны, поддержку политической оппозиции, провокацию протестных выступлений и социальных конфликтов, участие в тайных лонгитюдных операциях спецслужб.

6. *Национальные и международные научно-исследовательские и образовательные учреждения* (американский Брукингский институт,

британский Международный институт стратегических исследований и т. п.) — обеспечивают научно-методическую и информационно-аналитическую поддержку ведения ИПсВ, организуют научно-представительские мероприятия подрывного характера, обучают субъектов ведения ИПсВ, выступают в качестве источников информации для СМИ в ходе ведения ИПсВ.

7. *Международные религиозные экстремистские организации* (турецкая религиозная организация «Нурджулар», международные религиозные организации «Братья мусульмане», «Хизб ут-Тахрир аль-Ислами» и т. п.) — осуществляют идеологическую обработку населения, способствуя дестабилизации общества за счет обострения национальных и религиозных противоречий и провоцирования конфликтов. В контексте ИПсВ данные организации рассматриваются преимущественно как агенты спецслужб государств, выполняющие подрывную работу.

8. *Средства массовой информации* (американская Кабельная новостная сеть Си-эн-эн, Британская телевещательная корпорация Би-би-си, китайское Информационное агентство «Синьхуа» и т. п.) — преимущественно выступают в качестве агентов ведения массированной политической и военной пропаганды государственных органов, проведения лонгитюдных операций специальных служб, но могут иметь и собственные цели в ИПсВ.

9. *Индивидуальные сетевые активисты и их объединения* (Эдвард Сноуден, группа «Anonimus», активисты проекта «WikiLeaks» и т. п.) — участвуют в ведении ИПсВ войны как индивидуально, так и совместно с правительственными органами³⁴ посредством

³⁴ Важно отметить, что сетевые активисты не обязательно действуют в интересах государственных органов страны пребывания. Они могут действовать и против них в соответствии со своими целями и убеждениями.

кибератак на сайты, пропагандистской деятельности в Интернете и офлайн реальности, контрпропаганды против враждебных блогеров и т. д.

Основные направления ИПсВ

Вопрос о направлениях ИПсВ является одним из наименее разработанных. В имеющейся литературе по означенной проблеме он часто остается вне поля внимания авторов, которые фокусируются преимущественно на средствах и методах ведения ИПсВ. Проанализируем встречающиеся подходы и представим собственное видение вопроса.

А. В. Бедрицкий со ссылкой на авторитетного американского эксперта М. Либицки выделяет в американской доктрине ИВ четыре «категории информационно-психологических операций, проводимых в рамках психологической борьбы»:

- операции против структур государственного управления;
- операции против структур военного командования;
- операции по деморализации личного состава вооруженных сил;
- война культур (*нем.* Kulturkampf).

В качестве критерия классификации здесь выступают объекты ИПсВ. Но если первые три направления вполне укладываются в базовую концепцию ПсО вооруженных сил США, то последнее носит весьма специфичный характер. Оно адресовано обществу в целом и связано с влиянием на культуру страны или отдельные ее элементы.

Д. А. Волкогонов в своей работе писал о схожем с «войной культур» типе акций — *идеологических диверсиях* (далее — ИД). Под ИД он понимал «конкретную духовную акцию, направленную против социалисти-

ческого общественного сознания с целью изменения в нем жизненных установок и ориентаций». При этом автор отмечал, что такие диверсии осуществляются как в теоретической плоскости (искажение методологических положений марксизма-ленинизма, фальсификация исторических концепций, извращение принципов права, этики и др.), так и в психологической (муширование заявлений различных отщепенцев, фабрикация политических фальшивок, популяризация различных антисоветских сборищ и т. п.)³⁵. Поддерживая точку зрения автора, вместе с тем полагаем неудачным сам термин «ИД», поскольку лежащее в ее основе понятие «идеология» характеризует уровень теоретического сознания, тогда как содержание «ИД» предполагает и диверсии, направленные против обычного сознания.

В качестве примера, доказывающего реальность ИД и стоящих перед ними целей, автор приводит слова заместителя директора «Голоса Америки» Ф. Николайдеса, который, комментируя установки Вашингтона по ПсВ, заявил в начале 1982 года: «Мы должны дестабилизировать Советский Союз и его союзников, способствуя разладу между народами и правительствами. Нужно расшатать изнутри то, что составляет содержание марксистских взглядов и убеждений»³⁶. В профильной литературе широко цитируется так называемая Доктрина Аллена Даллеса (А. Даллес — бывший директор ЦРУ), описывающая методику ПсВ против СССР с выделением тех же элементов, которые Д. А. Волкогонов идентифицировал как ИД. Несмотря на наличие обоснованных сомнений в аутентичности самой на-

³⁵ См. Д. А. Волкогонов. Психологическая война. С. 106–107.

³⁶ Там же. С. 108.

званной «доктрины», анализ хроники ПсВ войны США против СССР, проведенный исследователями³⁷, однозначно подтверждает, что указанные в ней направления и методы ПсВ многократно применялись на практике и доказали свою эффективность.

Следует отметить, что существование рассматриваемого «культурно-идеологического» направления ПсВ было признано и на высшем политическом уровне. Очень четко о нем было сказано Президентом России В. В. Путиным в ходе встречи с пред-

Попытки влиять на мировоззрение целых народов, стремление подчинить их своей воле, навязать свою систему ценностей и понятий — это абсолютная реальность, так же, как борьба за минеральные ресурсы, с которой сталкиваются многие страны, в том числе и наша страна

ставителями общественности по вопросам патриотического воспитания молодежи в Краснодаре в 2012 году: «Как показывает в том числе и наш собственный исторический опыт, культурное самосознание, духовные, нравственные ценности, ценностные коды — это сфера жесткой конкуренции, порой объект открытого информационного противоборства, не хочется говорить «агрессии», но противоборства — это точно, и уж точно хорошо срежиссированной пропагандистской атаки. И это никакие не

³⁷ См.: В. А. Лисичкин, Л. А. Шелепин. Третья мировая информационно-психологическая война. М., 2003; И. Н. Панарин. Первая мировая информационная война. Развал СССР. СПб., 2010.

фобии, ничего я здесь не придумываю, так оно и есть на самом деле. Это как минимум одна из форм конкурентной борьбы. *Попытки влиять на мировоззрение целых народов, стремление подчинить их своей воле, навязать свою систему ценностей и понятий — это абсолютная реальность*, так же, как борьба за минеральные ресурсы, с которой сталкиваются многие страны, в том числе и наша страна»³⁸.

Рассматривая подходы к выделению направлений ИПсВ, необходимо выделить шесть ключевых приоритетов управления.

При применении их одной социальной системой по отношению к другой они рассматриваются как «обобщенное оружие», то есть средства ведения войны. Ранжирование приоритетов в данном случае осуществлено по критерию силы воздействия на общество на исторически длительных интервалах времени: первый является наиболее, а шестой — наименее мощным. При этом показатели быстроты получения эффекта воздействия обратно пропорциональны положению в списке.

Шесть выделенных приоритетов управления достаточно адекватно охватывают спектр существующих методов ведения противоборства между государствами. Причем в отличие от шестого, традиционного (военного) способа борьбы остальные носят невоенный характер. В последнее время исследованию этих способов уделяет-

³⁸ «Встреча с представителями общественности по вопросам патриотического воспитания молодежи. Краснодар, 12 сентября 2012 г». — <http://kremlin.ru/news/16470>.

ся большое внимание в литературе, в части из которой для их обозначения используется понятие «организационное оружие»³⁹. Однако нас интересуют только три первых из них, которые носят информационный характер и могут быть отнесены к ИПсВ.

В качестве актуального примера применения «хронологического приоритета» можно привести компьютерную игру «Компания героев 2» (Company of Heroes 2), выпущенную летом 2013 года канадской компанией «Relic Entertainment» и посвященную событиям на Восточном фронте Второй мировой войны. В ней советские войска изображены в крайне негативном виде: они проявляют трусость и жесткость (добивают пленных, сжигают деревни с мирными жителями и т. д.), используют своих солдат как «пушечное мясо», широко применяют заградотряды для пресечения дезертирства с поля боя и т. д. Например, в одной из миссий игры всплывает подсказка: «Не бойтесь жертвовать новобранцами. Советская доктрина считала, что для достижения тактических или стратегических целей это вполне допустимо». Сам главный герой, один из командиров Советской армии, находится по сюжету игры в ГУЛАГе, откуда и вспоминает «кровавые события» Великой Отечественной войны. При этом разработчики игры заявляют об исторической достоверности событий, положенных в основу игры⁴⁰.

³⁹ См.: «Оргоружие: о том, что хаос может быть рукотворным. Сводная аналитическая группа Центра Кургиняна об угрозах суверенитету России». М., 2007; **В. И. Якунин, В. Э. Багдасарян, С. С. Сулакшин**. Новые технологии борьбы с российской государственностью. М., 2009; **В. С. Овчинский, И. Ю. Сундиев**. Организационное оружие: Функциональный генезис и система технологий XXI века (доклад Изборскому клубу). — «Изборский клуб. Русские стратегии». 2013. № 6.

⁴⁰ См. «Российские геймеры вступились за честь Красной Армии». 27.07.2013. — <http://russian.rt.com/article/13095>

Еще одна заслуживающая внимания классификация направлений ведения ИПсВ представлена С. Кургиняном⁴¹. Автор, апеллируя к общей теории систем, называет следующие способы разрушения системы:

- деформация, вплоть до деградации, целевых функций системы;
- искажение целевых приоритетов;
- разрыв или «переключение» системных управляющих связей;
- обострение внутрисистемных противоречий как в целеполагающем ядре системы, так и между ее ядром и подсистемами;
- раскачка «автоколебаний» системы для ее вывода за пределы устойчивости.

Говоря о применимости данных методов и к социальным системам, С. Кургинян вводит понятие *оргвойны*, которое он определяет как нужное атакующему управление мотивациями организационных решений противника во всех частях его социально-государственной системы. Как видно, автор делает ключевой акцент на влиянии на целеполагание управленческого ядра системы (то есть политического руководства страны). Данное направление ИПсВ представляется нам одним из ключевых.

Среди способов воздействия на противника С. Кургинян называет и создание иллюзии благополучия, блокирующей использование мобилизационных защитных механизмов⁴².

С учетом вышеизложенного представим авторское видение *основных направлений ИПсВ*, к которым, на наш взгляд, относятся:

- психологические операции против войска и населения противника в ходе войны или в угрожаемый период;

⁴¹ См. **С. Кургинян**. Ода страху. О праве оперировать понятием «оргоружие». — «Оргоружие: о том, что хаос может быть рукотворным». С. 5.

⁴² См. там же. С. 5—6.

— психологические операции, воздействующие на процесс целеполагания и выработку решений политическим и военным руководством страны в мирное и военное время;

— информационное противоборство в сфере истории;

— психологические операции в сфере культуры, воздействующие на менталитет, культуру и ценностно-нормативную систему общества;

— подрывные психологические операции, воздействующие на социальные связи и политическое поведение.

Организационные формы ведения ИПсВ

Помимо названных направлений считаем целесообразным выделить *организационные формы ведения ИПсВ*. Речь идет об определенных формах организации деструктивного информационно-психологического воздействия против государства, прообразом которых стала американская система стратегической коммуникации (Strategic Communication)⁴³, включающей несколько обособленных форм: связи с общественностью (Public Affairs), публичную дипломатию (Public Diplomacy) и информационные операции (Information Operation). При этом, в отличие от стратегической коммуникации, адресованной как внутренней, так и зарубежной аудитории, ИПсВ направлена только на вторую. Поскольку мы опирались на американскую концепцию, наряду с русскоязычными терминами в скобках укажем их англоязычные аналоги, употребляемые в официальных актах США.

⁴³ См.: «White House 2010. National Framework for Strategic Communication». — www.fas.org/man/eprint/pubdip.pdf; **Е. Н. Пашенцев**. Стратегическая коммуникация США: «Имперское перенапряжение сил». — «Мир и политика». 2012. № 8.

Итак, к числу *основных организационных форм ИПсВ* следует отнести:

1. *Психологические операции военного назначения (Military Information Support Operations)* — операции, направленные на оказание информационно-психологического воздействия на политическое и военное руководство страны, личный состав вооруженных сил и гражданское население, осуществляемые в угрожаемый период или во время вооруженного конфликта в целях содействия решению военных задач (деморализация противника, принятие ошибочных решений руководством страны-противника, обеспечение поддержки действий своих вооруженных сил членами международного сообщества). Проводятся специализированными подразделениями вооруженных сил (армии, ВМФ, ВВС), иных военизированных формирований при поддержке гражданских внешнеполитических ведомств.

2. *Публичную дипломатию (Public Diplomacy)* (ПД) — совокупность методов информационного влияния на общественное мнение зарубежных государств и международного сообщества в целях реализации политических, дипломатических и военных задач. В качестве основных задач ПД выступает улучшение международного имиджа страны, влияние на элиту зарубежных стран, улучшение экономического и инвестиционного климата для национального (и связанного со своей страной транснационального) бизнеса в зарубежных странах⁴⁴. ПД является основным способом реализации так называемой мягкой силы (soft power).

⁴⁴ См.: **А. И. Кубышкин, Н. А. Цветкова**. Публичная дипломатия США. Учебное пособие для вузов. М., 2013. С. 50–51; **Р. С. Мухаметов**. Роль публичной дипломатии в формировании международного имиджа России. — http://community.livejournal.com/image_of_russia/62907.html

er) и включает внешнеполитическое информирование, образовательные и научные обмены, программы в области культуры и науки, иные формы гуманитарного сотрудничества. ПД реализуется специальными государственными учреждениями публичной дипломатии или подразделениями иных государственных органов (ведомств иностранных дел, национальной безопасности и др.) при активном участии неправительственных организаций, образовательных и научно-исследовательских структур, СМИ.

3. *Внешнеполитическую пропаганду (Propaganda)* — распространение взглядов, идей и теорий с целью формирования у масс определенного мировоззрения, представлений, отражающих интересы субъекта пропаганды, и стимулирования соответствующих им практических действий⁴⁵. Пропаганда как метод информационно-психологического воздействия активно применяется в публичной дипломатии и военных психологических операциях. Вместе с тем она может быть выделена и как обособленная форма ИПсВ для обозначения деятельности государственных органов и СМИ по оказанию информационно-психологического воздействия на зарубежную аудиторию. Как форма ИПсВ может также включать и воздействие на собственное население в целях умышленной дискредитации в общественном мнении определенного иностранного государства. Пропаганда осуществляется перманентно и с течением времени меняет лишь свою интенсивность и направленность.

4. *Тайные психологические операции специального назначения (Covert*

Operations) — операции тайного характера, проводимые в целях вмешательства во внутренние дела другого государства для дестабилизации обстановки в нем, провокации социальных конфликтов, протестных выступлений, а также оказания воздействия на культуру и ценностно-нормативную систему общества. Их можно подразделить на тактические подрывные ПсО (психологические диверсии) и стратегические лонгитюдные ПсО. Основную роль в их проведении играют специальные службы государства. Важной особенностью является активное вовлечение в их реализацию определенных лиц, групп людей или общественных институтов, являющихся гражданами (резидентами) государства—объекта ИПсВ, которые были предварительно завербованы или участвуют в ПсО против своей страны добровольно (агентура влияния, или «пятая колонна»). Рассматриваемый тип психологических операций является наиболее закрытой, трудно выявляемой и опасной формой ИПсВ.

Для ведения ИПсВ применяется чрезвычайно обширный арсенал средств и методов, для обозначения которого используется понятие *информационное оружие*, или более точно — *информационно-психологическое оружие*. Под последним В. Ф. Прокофьев понимает «совокупность способов и средств (технологий) открытого (или полускрытого) воздействия на психику людей, применяемая в ходе информационно-психологической борьбы (войны) для достижения поставленных целей»⁴⁶. Рассмотрение всего их многообразия в рамках настоящей статьи не представляется возможным.

⁴⁵ «Пропаганда». — «Большая советская энциклопедия». В 30 т. М., 1969—1978. Т. 21. — <http://bse.sci-lib.com>

⁴⁶ В. Ф. Прокофьев. К проблеме формирования основных понятий в области информационной безопасности. С. 241.

Для «пунктирного» обозначения многообразия информационно-психологического оружия перечислим основные методы и средства ИПсВ, отраженные в ключевых работах по исследуемой проблематике. Так, к числу методов ПсВ Д. А. Волкогонов отнес следующие: манипуляцию сознанием, дезинформацию, запугивание, распространение слухов, «кражу лозунгов», создание иллюзорных стереотипов мышления, «подтасовку карт», «наклеивание ярлыков» и др.⁴⁷ В. Ф. Прокофьев подразделяет методы ИПсВ на две группы:

— с использованием «чистых» технологий: убеждение, глубокая проработка предложений по решению проблемы, личный пример, выполняемые обещания и клятвы, научно-обоснованный прогноз развития событий и др.;

— с использованием манипулятивных («грязных») технологий: метод стереотипизации, ложь, навешивание ярлыков, сияющие обобщения, перенос или трансфер, игра в простонародность, осмеяние, продвижение через авторитетов и др.

Что касается средств ведения ИПсВ, то их палитра еще более разнообразна и простирается от подпольной «самиздатовской» брошюры до телерадиовещательных комплексов воздушного базирования, используемых в армейских психологических операциях⁴⁸. Г. Г. Почепцов в качестве

инструментария ПсО называет: листовки, громкоговорители, радиовещание, слухи, Интернет, общение лицом к лицу⁴⁹.

Заключительные замечания

Завершая рассмотрение феномена информационно-психологической войны, отметим, что вопросы противодействия ей требуют отдельного изучения. Следует подчеркнуть, что всякого рода правовые и иные запреты на ведение ИПсВ имеют весьма сомнительные перспективы реализации. Апелляции к соблюдению принципа невмешательства во внутренние дела государства и иным основополагающим принципам международного права звучат весьма благородно и справедливо, однако они не способны предотвратить применение методов информационно-психологического противоборства против нашей страны. Выход в этой ситуации нам видится один: научиться вести информационно-психологическую войну и создать для этого необходимый потенциал («capacity building»), дабы обеспечить надежное сдерживание потенциально агрессивора и достойный отпор враждебным психологическим операциям. ◆

⁴⁷ См. Д. А. Волкогонов. Психологическая война. С. 120—135.

⁴⁸ Такими комплексами оснащены самолеты радиоэлектронной борьбы ЕС-130Е (RR, J), стоящие на вооружении 193-го авиокрыла специальных операций ВВС США. Они обеспечивают трансляцию и ретрансляцию с воздуха на территории противника радио- и телевизионных программ. См. «Информационные, специальные, воздушно-десантные и аэромобильные операции армий ведущих зарубежных государств». С. 43—44.

⁴⁹ См. Г. Г. Почепцов. Психологические войны. М., 2002. С. 443—457.