Международные процессы, Том 13, № 2, сс. 141–145
DOI 10.17994/IT.2015.13.2.41.10

SCRIPTA MANENT
Рукописи не горят. Рецензии

ЦИФРОВОЙ И БЕЗОПАСНЫЙ?

Глобальная безопасность в цифровую эпоху: новые стратагемы для России / Под общей редакцией А.И. Смирнова М.: ВНИИгеосистем, 2014. 394 с.

По мере роста значимости в современной международно-политической повестке дня проблем информационной безопасности, данная тематика оказывается в фокусе все более широкого круга научных, учебных и беллетристских публикаций. Вместе с тем даже на фоне обостряющейся конкуренции изданий в этой предметной области книга *«Глобальная безопасность в цифровую эпоху: новые стратагемы для России»* выделяется по широте рассматриваемых вопросов и практико-ориентированной направленности.

В ней нашли отражение характерные черты цифровой эпохи, острые угрозы Интернет-пространству на глобальном и региональном уровне, место России в этом сегменте международного соперничества. Новые тенденции развития информационной сферы рассматриваются на примерах совсем недавних «цветных революций», а также событий на Украине, что повышает актуальность проведенного анализа. Авторский коллектив, представленный А.И. Смирновым, В.Р. Григорьевым, И.Н. Кохтюлиной, Б.В. Куроедовым и О.В. Сандаровым, задался целью подробно изучить особенности современного этапа внедрения информационно-коммуникационных технологий (ИКТ) в общественную и политическую жизнь, оценить сетевую мощь государств, выявить и систематизировать основные вызовы международной информационной безопасности, пути их анализа и прогнозирования.

Первая глава издания посвящена *мегатрендам цифровой эпохи*. В ней рассматривается эволюция технологических укладов, сопоставляются страны по степени развития ИКТ и доступу к ним населения. Авторы знакомят читателей с методологией анализа социальных сетей как эффективным инструментом изучения взаимодействий в информационной сфере.

Характеризуя современный этап глобального развития, исследователи высвечивают начавшийся переход к шестому технологическому укладу, который качественно отличается от всех предыдущих. В процессе его становления новым драйвером прогресса выступает не столько экономический потенциал, сколько интеллектуальные способности индивида. В этой связи растущее значение приобретают НБИК-технологии (нано, био, информационные и когнитивные), которые способствуют преобразованию ресурсного потенциала в интеллектуальные производительные силы в различных сферах деятельности. То государство, которое сможет овладеть этими технологиями в промышленном масштабе, и будет определять будущее мировой политики, заключают авторы.

Между тем становление глобального информационного пространства характеризуется значительной неравномерностью. К концу 2013 г. 2,7 млрд человек были подключены к сети Интернет, что составляло 40% населения мира. В то же время анализ ситуации на уровне отдельных обществ свидетельствует о сохранении значительного цифрового неравенства – при построении политической карты информацион-

ного пространства привычные контуры стран существенно сдвигаются.

Во второй главе речь идет *о геополитических вызовах в новой эпохе* информационных технологий. Сопоставляя силу и влияние ведущих центров современного мира, авторы привлекают особое внимание к оценкам сетевой мощи государств. Применительно к России авторы заявляют о том, что её влияние эквивалентно «среднему уровню сверхдержавы» (с. 57) – меньше всего влияние нашей страны прослеживается в экономической области из-за недостаточного присутствия на технологических рынках, а также в военной сфере, несмотря на ядерный потенциал. Китай превосходит Россию по большинству показателей, но уступает в степени военного влияния.

Евросоюз, по заключению авторов, постепенно укрепляет свои позиции в мировой табели о рангах и вскоре сможет претендовать на статус коллективной сверхдержавы. Вместе с тем до сих пор абсолютным лидером по всем показателям остаются США, вполне подтверждая свой сверхдержавный статус. Если по ряду критериев, например, в области экономического влияния, с США могут конкурировать и ЕС, и Китай, то в военной сфере Америке равных нет.

В этой же главе авторы предлагают беглый прогноз перспектив изменения текущей ситуации в результате развития региональных и глобальных интеграционных процессов, однако даже укреплённым ШОС и Евразийскому Союзу будет сложно соперничать с НАТО по уровню международной влиятельности. На наш взгляд, тема прогнозирования дальнейшего изменения геополитической ситуации в мире заслуживает более детальной проработки в формате отдельного исследования.

Информационные технологии не только создают новые возможности, но и представляют опасность для мирового сообщества, суверенитета отдельных государств, их стратегических объектов. В этой связи проблематика международной информационной безопасности (МИБ) стала предметом рассмотрения третьей главы. Ключевую роль в ее укреплении на протяжении длительного времени играет Российская Федерация, выдвигая различные инициативы по линии Генеральной Ассамблеи ООН. Не без ее участия, например, в 2004 г. была учреждена Группа правительственных экспертов ООН, призванная стать площадкой обмена профессиональными мнениями в области информационной безопасности, поиска компромиссных подходов в сфере ее политико-правового регулирования. Этот международный орган занимается изучением вопросов, связанных с использованием информационных технологий в конфликтах и с применимостью норм международного права по отношению к этому пространству.

Авторы издания отмечают, что российская дипломатия в ее усилиях по укреплению МИБ концентрируется на нескольких направлениях. *Во-первых*, она стремится к выработке документов, обеспечивающих регулирование действий государств в области использования ИКТ. Знаковой инициативой в этой области стал проект Конвенции об обеспечении МИБ, предложенный Россией для международного обсуждения. *Во-вторых*, она добивается налаживания двустороннего сотрудничества. Например, был достигнут серьёзный прогресс во взаимодействии с США, которые признали значимость проблем, связанных с использованием ИКТ государствами в военно-политических целях. *В-третьих*, Москва осознает необходимость совершенствования национального законодательства и доктринальных установок. Так, в России уже внесён ряд поправок в нормативные документы: вопросы МИБ нашли отражение в новой Концепции внешней политики России от 12 февраля 2013 года. Отдельное внимание авторы книги уделили «Основам государственной политики РФ в области международной информационной безопасности на период до 2020 года», в которых даётся развёрнутое толкование МИБ, определяются основные положения стратегии Российской Федерации в этой сфере.

В издании отмечаются сложности в обеспечении МИБ, обусловленные разницей в западном и российском подходах к этой проблематике. Например, в 2013 г. было опубликовано «Таллиннское руководство» по ведению кибервойн НАТО, оценённое рядом экспертов как элемент обоснования легитимности такого средства международной борьбы. Между тем, с точки зрения российской стороны, само развертывание подобного рода конфликтов в информационной сфере представляется недопустимым.

Особый интерес представляют четвертая и пятая главы книги, поскольку в них предпринимается попытка практического применения теоретических знаний о сетецентричных войнах. В частности, рассматриваются основные черты «цветных революций», в которых используются технологии «мягкого перехвата власти». Использование стратегии сетецентричного конфликта, понимаемого в терминах войны, в которой происходит концентрация всех имеющихся ресурсов (информационных, политических, экономических, военных) с целью поражения потенциального противника, становится одной из характеристик происходящей «революции в военном деле». По мнению авторов, в настоящее время наблюдается расширение использования методов сетецентричной войны Соединенными Штатами до масштабов глобальной информационной агрессии.

Сегодня противостояние в информационной среде разворачивается не только между государствами, но и между неправительственными организациями. С учетом того обстоятельства, что с сетецентричными структурами можно бороться только с помощью аналогичных инструментов, предпочтение отдается *невоенным операциям*. Так, например, США организуют тесное взаимодействие между подразделениями вооруженных сил и гражданскими государственными и неправительственными организациями, активно используют гуманитарные фонды и неформальные объединения для создания подконтрольных политических, экономических и социальных сетевых объединений, которые могут быть задействованы при создании необходимой информационной и организационной обстановки для легитимной передачи власти. В этой связи в книге раскрывается феномен «цветных революций» как пример такого рода деятельности.

В развитие этой тематики в пятой главе анализируется информационная сторона событий, происходивших на Украине в 2013–2014 годах. Приводится любопытная информация, которая указывает на участие США в поддержке «Евромайдана». Помимо оказания финансовой помощи оппозиционным силам, Соединенные Штаты через каналы Государственного департамента и Агентства по международному развитию развернули информационную борьбу в сети Интернет. На наш взгляд, для полноты картины стоило проанализировать не только примеры зарубежного участия в информационной войне на Украине, но и посмотреть, какие контрмеры принимали российские спецслужбы.

Разоблачение Э. Сноуденом американской глобальной системы слежения, описанное в шестой главе, свидетельствует о том, что развитие ИКТ технологий может иметь деструктивное влияние не только на международную политику, но и на общественное сознание. Сегодня развернулась острая полемика о том, допустимо ли вмешательство в частную жизнь, массовая тайная слежка за гражданами для обеспечения национальной безопасности. В работе подробно проанализированы программы глобального сбора информации, используемые спецслужбами США и других стран, а также рассмотрены основные партнеры и объекты интереса Агентства национальной безопасности Соединенных Штатов.

В книге поднимаются такие актуальные вопросы, как необходимость соблюдения права на неприкосновенность личной жизни в онлайн-пространстве и ограничения продажи систем слежения за Интернет-трафиком и программ сбора метаданных. Сегодня для государств становится все более важным гарантирование кибербезопасности с учетом подверженности элементов

национальной информационной инфраструктуры деструктивному внешнему воздействию со стороны как иностранных правительств, так и негосударственных участников.

От изучения отдельных примеров и проблем в области МИБ авторы переходят к изложению методологии анализа взаимодействий в информационной сфере. В рамках научного подхода к исследованию этой проблематики они выделяют четыре направления: геополитическое, бихевиористское, интерактивное и системное. Каждому из них даётся характеристика, выявляются их наиболее существенные недостатки. В частности, при описании интерактивного подхода анализируются основы теории игр, теории торга, а также моделирования.

Авторы акцентируют внимание читателей на особенностях изучения международных информационных конфликтов. В этой связи выделяют его основные структурные компоненты: участники, их интересы и ресурсы, цели. Что касается ранжирования конфликтов, то для оценки их сравнительной значимости предлагается оригинальная матрица сопоставления. В книге также содержится авторская типология конфликтов.

Инновационный характер недавних вооруженных столкновений определяется их ориентацией на размывание государственных структур. Новые войны характеризуются большей продолжительностью и масштабами, в них, как правило, нет явных «победителей» и «побежденных». Помимо этого, меняются и сами действующие лица – в современных конфликтах возникает целый класс боевиков, сознание которых качественно отличается от представлений обычных военнослужащих. Они не заинтересованы в мире, не имеют каких-либо перспектив в послевоенной жизни и представляют собой серьезную угрозу для общества.

С учетом трансформации природы конфликтов современные методики их исследования также меняются – они заимствуют инструментарий изучения конкуренции между фирмами в экономике и менеджменте. В частности, все большее распространение приобретают SWOT и STEEPLE анализ. Первая методика направлена на выявление сильных и слабых сторон объекта изучения, а также возможностей и угроз для него из внешней среды. STEEPLE-анализ направлен на комплексное изучение основных факторов среды, в которой разворачивается конфликт: в том числе социально-демографического, экономического, политического, экологического. Авторы приходят к выводу, что одним из наиболее эффективных методов изучения конфликтов остается и традиционный ситуационный анализ.

В то же время в современных условиях появляется возможность повысить его продуктивность путем встраивания в работу ситуационно-кризисных центров, благодаря которым можно добиться нового качества оперативного прогнозирования. Появление таких центров стало косвенным результатом информационной революции. В книге приводятся характеристики *ситуационно-кризисных центров* в ряде стран – в том числе в ФРГ, Италии, России.

В завершающей главе авторы сосредоточивают внимание на значении и роли «мягкой силы» в современных международных отношениях. Само это понятие, введенное американским исследователем Дж. Наем, сегодня преобразовывается в соответствии с меняющимися реалиями, в том числе с учетом развития ИКТ. В работе выделяются критерии составляющих «мягкой силы» и проанализирован рейтинг ее использования по странам. Кроме того, рассматривается влияние ИКТ на внешнеполитический инструментарий государств с учетом появления механизмов электронной дипломатии. В издании подробно рассмотрены основные составляющие электронной дипломатии США, Великобритании и Германии.

В заключение авторы приходят к выводу о том, что национальная информационная безопасность неотделима от международной, поэтому России необходимо продолжать настаивать на реализации инициатив в области МИБ, обеспечивающих интернационализацию глобального информацион-

ного пространства. Попытки применения ИКТ в целях, противоречащих задачам обеспечения международной и национальной безопасности, должны пресекаться мировым сообществом, в том числе ООН. Эта организация сегодня, больше чем когда-либо, востребована в качестве основной площадки для обсуждения проблем МИБ. Россия при осуществлении своей внешней политики должна добиваться такого состояния глобальной информационной среды, при котором не будут нарушаться права личности, общества и государств, а также будут исключены возможности разрушительного внешнего воздействия на национальное информационное пространство.

Анна Макарычева,
Татьяна Дроздова