визового режима между РФ и странами – участницами ЕС и подписание двустороннего Соглашения.

Понимая опасения восточноевропейских государств, Германия тем не менее пытается избежать резких высказываний и действий, которые могли бы спровоцировать Россию. История наглядно демонстрирует отсутствие прецедентов того, что санкции изменили бы ментальность руководства страны, против которой они были направлены. Германия привыкла за долгие десятилетия решать проблемы дипломатическим путем, и кроме того, жесткий тон на внешнеполитической арене не найдет поддержки у населения ФРГ. Однако следует учитывать и то, какое значение для немцев сейчас имеют германо-польские отношения. Польша, являющаяся главным торговым партнером Германии в Европе, находится на положении привилегированного партнера, и это четко продемонстрировала германо-польская инициатива в ходе дипломатических усилий по урегулированию кризиса в Украине. С точки зрения экономической выгоды Германия будет, пожалуй, периодически играть на стороне Польши, однако одновременно среди германской политической и экономической элит существует широкий консенсус относительно того, что Россию нельзя исключать из различных международных «клубов» и переговорного процесса, дабы избежать маргинализации ее внешней политики в условиях международной изоляции.

В целом граждане ФРГ оценивают внешнеполитическую активность своего правительства более чем положительно. Согласно последним данным социологических опросов в Германии, работой федерального правительства довольны 47% немцев, при этом деятельностью МИД ФРГ довольны 67% респондентов (28% оценивают ее отрицательно), 74% немцев поддерживают действия Ф.-В. Штайнмайера, 71% – А.Меркель, 47% – министра обороны У. фон дер Ляйен[1].

Де-юре европейские страны просто не могут, и никогда не смогут признать итоги и законность Крымского референдума, этот шаг означал бы для них появление в Европе дамоклова меча – возможности нарушения государственных границ на континенте в одностороннем порядке. В данной ситуации мы можем говорить о том, что Германия, пребывавшая в статусе особого партнера РФ, «моста» между ЕС и Россией, тесно связанная экономическими интересами с нашей страной, оказалась в самой сложной ситуации среди своих европейских коллег. Разумеется, немцам придется в какой-то мере поступиться своими экономическими интересами и проявить европейскую и атлантическую солидарность, попытавшись при этом снизить, по возможности, размер собственного ущерба.

Строить сценарии и прогнозы развития ситуации в Украине и вокруг Крыма можно до бесконечности, однако уже сейчас очевидно, что одним из главных результатов кризиса стало «рождение» подлинно единой Европы, которая, несмотря на разную ментальность, исторический опыт, экономические условия, сомкнула ряды перед лицом того, что европейские государства восприняли как угрозу своей ценностной идентичности. И Германия сохранила и преумножила в этой ситуации свою позицию лидера обновленной Европы, которая смогла преодолеть в глобальном плане раскол на «старо» и «младоевропейцев».

[1] www.tagesschau.de/inland/deutschland/trend/2174.html

БЕЗОПАСНОСТЬ В КИБЕРПРОСТРАНСТВЕ: НА ПУТИ К СОТРУДНИЧЕСТВУ

Сергей Кулик,
директор по проблемам международного развития,
Институт современного развития

Тема безопасности в киберпространстве уже вышла на первый план в глобальной и региональной повестках. Ее обсуждали на прошедшей Мюнхенской конференции по безопасности 2014 г., впереди – специализированные саммиты, начиная с проводимого в Бразилии в апреле мероприятия в рамках ООН, международный конгресс Всемирного союза электросвязи и др. Все громче звучат голоса экспертов, призывающих НАТО детально обсудить эту проблему на сентябрьском саммите.

В середине января американский «Дефенс ньюс» опубликовал результаты опроса представителей исполнительной и законодательной властей США, занимающихся проблематикой национальной безопасности. Впервые доля обеспокоенных вызовами из киберпространства превысила долю тех, кто на первое место выносит террористическую угрозу. Причем почти в два раза.

В последнее время все большую озабоченность демонстрирует руководство многих ведущих стран, в убыстренном темпе приступивших к принятию «стратегий кибербезопасности». Вслед за США, Великобританией, Канадой и Германией только в 2013 г. несколько государств в Европе и за ее пределами одобрили такие стратегии.

В свою очередь, Россия обновила свою позицию в «Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». В ней отражена растущая тревога по поводу ситуации и перспектив ее развития на этом направлении.

С бурным ростом информационных и коммуникационных технологий (ИКТ) киберпространство стало трансграничным, от него во многом зависят интересы граждан, бизнеса и государственных ведомств, функционирование экономик и финансов. Соответственно,

ИКТ не только предлагают благоприятные возможности, но и повышают уровень опасностей для всей вертикали – от отдельного человека до национальных, региональных и глобальных механизмов.

Раньше внимание экспертов было сосредоточено преимущественно на вызовах безопасности для военной инфраструктуры и других критически важных объектов (например, атомных станций). С расширением списка объектов и участившимися случаями кибератак на иные адресаты, в том числе финансовые структуры, руководители ведущих государств начали признавать: вместе с различными сбоями в работе ИКТ это может оказывать негативное воздействие даже на темпы социально-экономического развития отдельных стран.

Новые технологии дают возрастающие возможности: поражать банковские системы, воздействовать на государственное управление, вызывать техногенные катастрофы, взламывать коды важных объектов. А без должного международного сотрудничества весьма сложно определить источник такого рода кибердаров. Не удивительно, что тема киберпространства все заметнее просматривается в повестках авторитетных международных форумов, занимающихся темами, далекими от традиционных вопросов безопасности (в частности, «Группы двадцати»). В общем, необходимо разрабатывать международные «правила игры».

Для политиков и экспертов возникают новые задачи на стыках военных и невоенных вопросов. Одна из них – право государства на ответную реакцию, на использование силы в случае идентификации источников действий, скажем, против банковских структур с существенным ущербом для государства. Какой уровень ущерба достаточен для того, чтобы применение военной силы (и насколько масштабное) стало легитимным, т.е. получило одобрение мирового сообщества? Другими словами, речь идет об относительных новшествах в сфере конфликтологии.

Все это свидетельствует о необходимости расширения повестки и взаимодействия между ведущими мировыми игроками, и не только в рамках «клубов по интересам». На этом пути впереди много препятствий и разногласий, но, по нашему мнению, общая работа начинает приносить определенные плоды.

Для «наведения мостов» во благо формирования согласованных позиций ведущих игроков в киберпространстве уже довольно длительное время им приходится заниматься, на первый взгляд, простой и скучной проблемой. Она заключается в различном понимании и использовании терминологии. Западные государства предпочитают «кибербезопасность», а Россия вместе с некоторыми партнерами – «информационную безопасность» и «международную информационную безопасность» (МИБ).

Попытки расшифровать друг другу собственное видение занимали значительное время на политических и экспертных площадках, затрудняя достижение консенсуса. Западные собеседники больше отталкиваются от национальных рамок безопасности и от более предметного видения объектов и субъектов обеспечения безопасности – элементов соответствующей инфраструктуры Сети. Что касается международного измерения, то их предпочтения в основном сосредоточивались на вопросах регулирования Интернета.

Россия и некоторые ее сторонники, делая акцент на МИБ (определение, запущенное в официальный оборот еще в конце прошлого века с тогдашним уровнем развития сетевых технологий), предлагали относительно размытые формулировки, которые сохраняются и по сей день. Речь идет о международном информационном пространстве, в котором не нарушаются права личности, общества и государства в информационной сфере.

Несмотря на объяснения Россией МИБ, партнеры заподозрили ее в стремлении поставить информационные потоки под национальный контроль. А российские представители усмотрели в позиции собеседников прежде всего намерение сохранить существующий режим регулирования Интернета (с центральными серверами на американской территории). Фактически копья ломались преимущественно по поводу изменений статус-кво на этом поле. Однако тема безопасности в киберпространстве гораздо шире. К тому же список вопросов из-за развития ИКТ и сопутствующих ему угроз заметно пополняется. Поэтому достижение согласия в трактовке терминов становилось все более насущной проблемой.

Главное – без достижения определенного компромисса в терминологии сложно выработать конкретную повестку переговоров и программу действий. Вместе с тем разночтения и сосредоточенность на правилах регулирования Интернета прежде всего для «гражданских нужд» и общественных связей использовались как прикрытие для нежелания находить развязки и показатель степени заинтересованности одной или обеих сторон в формировании общих подходов.

После весьма продолжительных споров совсем недавно «лед, наконец, тронулся». В июне 2013 г. появилось «Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия». Речь идет об ИКТ. Впервые на таком уровне появилась формулировка – «угрозы безопасности в сфере использования ИКТ и самим ИКТ» и «борьба с ними».

Достигнутый терминологический компромисс позволил поставить более конкретные задачи, далеко выходящие за описанные выше рамки проблематики Интернета и его регулирования. Среди них – «более эффективная защита критически важных информационных систем», «урегулирование опасных ситуаций, вызываемых событиями, которые могут создавать угрозы безопасности в сфере использования ИКТ и самим ИКТ». Они, в свою очередь, сориентированы на противодействие «военно-политическим и криминальным угрозам, а также угрозам террористического характера». Не менее важно и то, что документ подписан руководителями стран, которые играют роль лидеров двух групп государств, предпочитающих либо «кибербезопасность», либо МИБ (к последней также тяготеют члены Шанхайской организации сотрудничества).

К сожалению, это событие на фоне других (Сирия, иранская ядерная программа и др.) получило незначительное отражение в мировых СМИ. Но оно представляется знаковым в качестве первого серьезного шага в сотрудничестве, и свидетельствует о том, что проблемы безопасности в киберпространстве становятся одним из приоритетов в российско-американских отношениях. Более того, договоренность можно оценивать как своего рода «пакт о ненападении».

Следует отметить, что она способствовала некоторым изменениям, которые вошли в российские «Основы», одобренные после Совместного заявления. На сей раз, помимо указанных выше размытых формулировок МИБ, в текст было добавлено положение о предотвращении «деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры». А это уже более предметно, ибо элементы вполне «осязаемы» и можно говорить о совместных международных усилиях по налаживанию нормальной работы.

Наконец, Совместное заявление дало сигнал для сдвигов и на международных переговорных площадках. Появились сообщения об интересе целого ряда государств, в том числе западных, к заключению аналогичных договоренностей с Москвой.

В декабре 2014 г. произошло еще одно знаковое событие. На встрече Совета министров иностранных дел ОБСЕ принят «Первоначальный перечень мер укрепле-

ния доверия в рамках ОБСЕ с целью снижения возникновения конфликтов в результате использования информационных и коммуникационных технологий». Российский МИД вполне справедливо отметил «прорывной характер документа». Действительно, в сфере укрепления доверия решение является беспрецедентным в истории Организации и охватывает уже все пространство от Ванкувера до Владивостока вместе со странами, которые ранее отстаивали более общие формулировки МИБ (например, Казахстан), либо делали акцент на «кибербезопасности». Определенный консенсус наконец-то найден, и теперь ОБСЕ будет (во всяком случае, пока) руководствоваться менее размытым термином «безопасность ИКТ и использования ИКТ».

Обратим внимание еще на один немаловажный акцент. В документе отмечается, что при дальнейшей разработке мер доверия ОБСЕ будет дополнять соответствующую деятельность ООН, а это подчеркивает значение, придаваемое центральной международной структуре. Раньше отсылки на нее в этой теме делались больше «для галочки». Но заметную активизацию ООН на данном направлении в последнее время стало труднее игнорировать.

По линии этой организации проводится действительно продуктивная работа. В ней заметна деятельность Группы правительственных экспертов, которая начинает играть ведущую роль в поисках компромиссов между крупными игроками с разными позициями. Собственно, она во многом помогла найти приемлемые формулировки и для Совместного российско-американского заявления, и для решений ОБСЕ. Накануне принятия заявления Группа выпустила свой второй доклад. В отличие от предыдущего, там говорится об «использовании ИКТ» – правда, в довольно ограниченном контексте предотвращения военно-политических конфликтов.

В этом отношении Совместное заявление пошло дальше доклада, ориентируя также на противодействие «криминальным угрозам» и «угрозам террористического характера». Тем не менее отход от «киберпространства» и от МИБ в формулировках Группы, куда входят эксперты из «разных лагерей» и доклад которой к тому же был составлен под председательством представителя Австралии, представляется важным событием. Заметим, что работа Группы продолжается, и нас ожидает очередной ежегодный доклад, где авторы должны более конкретно определиться с понятиями.

Вернемся к документу ОБСЕ. Он предлагает следующий график: для начала государства-участники на добровольной основе предоставят свои определения, касающиеся «безопасности ИКТ и использования ИКТ», с нужными пояснениями и конкретизацией терминологии. А на будущее – они «приложат усилия для составления согласованного словаря». В октябре 2014 г. планируется сформировать пакет вопросов и позиций для более детального обсуждения.

Естественно, что в отличие от двусторонних переговоров, достижение компромиссов в такой крупной организации, как ОБСЕ, представляется более сложным делом. Тем более что многочисленные национальные подходы придется вписывать в общую позицию. Но сравнивая это решение с предшествующими спорами вокруг терминологии, которые фактически блокировали выработку конкретной повестки целей и задач сотрудничества в сфере безопасности в киберпространстве, можно надеяться, что механизм приведен в действие.

Следует также отметить, что российско-американские договоренности и, в случае существенных подвижек, реализация решений ОБСЕ будут способствовать началу диалога между Россией и НАТО по этим вопросам. Пока обе стороны воспринимают данное направление работы без особого энтузиазма. Но осознание общего характера многих угроз из киберпространства и вероятные неожиданные «сюрпризы» со стороны ИКТ вполне могут сдвинуть этот диалог с мертвой точки. К этому полезно подготовиться заранее – прежде всего экспертному сообществу.

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКИ ЭФФЕКТИВНОГО РАЗВИТИЯ ПОТЕНЦИАЛА НАТО НА СОВРЕМЕННОМ ЭТАПЕ В РАМКАХ КОНЦЕПЦИИ «УМНОЙ ОБОРОНЫ»

Дмитрий Чижов,
научный сотрудник Отдела стратегических исследований ИМЭМО РАН

Современный этап трансформации Североатлантического альянса направлен на его адаптацию к новым, трансграничным угрозам. Для решения поставленных задач была выработана концепция «Умной обороны», которая будет определять и регламентировать процесс оптимизации имеющихся оборонных сил и средств в среднесрочной перспективе.

Проблематика оптимизации имеющегося потенциала и его дальнейшее развитие всегда были приоритетными для Североатлантического альянса. С момента создания НАТО накоплен большой опыт по развитию многонациональных оборонных сил и средств, объединению ресурсов и развитию оборонного потенциала. На сегодняшний день Североатлантический альянс очередной раз ставит перед собой задачу оптимизировать и сбалансировать свой потенциал, с тем чтобы он максимально отвечал текущим военно-техническим, военно-политическим и экономическим реалиям.

Современный уровень военно-технического развития стран – участниц НАТО, старение парка большинства систем вооружения и военной техники (ВВТ), значитель-