О предотвращении военных конфликтов в информационную эру[1]

Уважаемые коллеги!

По нашим оценкам, угроза возникновения военных конфликтов в результате агрессивного или иного враждебного использования информации и современных информационно-коммуникационных технологий (ИКТ) в последнее время существенно обострилась.

Она существует не только в воображении военных теоретиков, которые разрабатывают апокалипсические сценарии «мировой информационной войны» . В архивы уже вписаны имена целого ряда военных конфликтов, в которых ИКТ широко использовались для их развязывании и последующей эскалации.

Обратите внимание на то, как мировые СМИ отреагировали на операцию российских ВКС в Сирии. Как только по просьбе законного правительства Сирии она началась, на нашу страну обрушилась массированная пропагандистская атака. Некоторые публичные высказывания высоких должностных лиц ряда стран дают основания полагать, что ложь и искажение фактов стало основой их политической позиции. Покатился вал бесконечных обвинений российской стороны в «бомбежках жилых кварталов» и «гибели мирных жителей». Леденящие душу постановочные кадры заполонили Интернет и телевидение. В итоге мировое общественное мнение и сознание мировых политико-формирующих кругов постепенно стало дрейфовать в направлении «осознания» неотвратимости очередной крупной войны.

Следует отметить, что подобные методы пропаганды ранее неоднократно применялись в периоды военного обострения израильско-палестинского конфликта.

' Выступление подготовлено авторским коллективом в составе: Дылевский И.Н., Запивахин В.О., Комов С.А., Кривченко А.А.

[2] Ричард Кларк, Роберт Найк Третья мировая война. Какой она будет? Высокие технологии на службе милитаризма, Питер, 2011 г.

Возникает вопрос: «Как долго человечество будет мириться с тем, что безнаказанная ложь, распространяемая благодаря современным ИКТ по всему миру со скоростью света, ведет к различного рода междоусобицам, развязыванию агрессивных войн, массовой гибели ни в чем не повинных граждан, миграционной катастрофе, гибели целых государств, разрушению вековых ценностей мировой культуры?».

Мы знаем, что этот вопрос волнует не только нас. Например, США и их союзники также озабочены усилением угрозы возникновения военных конфликтов вследствие враждебного использования ИКТ. НАТО к своему июльскому саммиту в Варшаве готовит новую стратегию, призванную повысить эффективность реагирования на нетрадиционные угрозы, в том числе и угрозу информационной войны. При этом наиболее действенным ответом на нее считается метод «сдерживания» геополитических соперников[3], основанный на демонстрации, а при необходимости и применении, военной силы в информационном пространстве.

Полагаем, что реагирование военной силой на какие-либо реальные или мнимые информационные угрозы может серьезно дестабилизировать ситуацию во всем мире. Слишком много соблазнов «поиграть мускулами» в условиях, когда ежедневно и ежечасно неисчислимое множество компьютерных атак обрушивается на информационную инфраструктуру, а потоки экстремистских идей - на головы простых граждан.

К тому же, в очередной раз хочется напомнить, что даже воля 28 стран-членов НАТО не может узаконить применение статьи 51 Устава ООН (право на самооборону) в отношении угроз, исходящих из информационного пространства.

Для этого нужен глобальный консенсус, достичь которого можно только путем формирования **всеобъемлющей системы**

безопасности, как это было сделано в конце 80-х годов прошлого века[1].

В те непростые годы большинство государств-членов ООН пришло к пониманию того, что обеспечение всеобъемлющей безопасности возможно лишь на основе соблюдения **общепризнанных принципов международного права** (уважения суверенитета, политической независимости и территориальной целостности государств, отказа от интервенции и вмешательства во внутренние дела, неприменения силы или угрозы силой, мирного урегулирования споров, равноправия и самоопределения народов, уважения прав человека и основных свобод, сотрудничества между государствами, добросовестного соблюдения принятых ими обязательств в соответствии с Уставом ООН). При этом **механизм коллективной безопасности,** воплощенный в Уставе ООН, был признан фундаментальным и незаменимым инструментом для сохранения международного мира и безопасности. Эффективное функционирование этого механизма должно дополняться усилиями государств мирового сообщества по всемерному ограничению гонки вооружений и снижению уровня военного противостояния. В свою очередь, решение этих задач немыслимо без **укрепления доверия** между государствами на основе преодоления конфронтационных подходов, укрепления норм цивилизованного поведения и атмосферы гласности и открытости в международных отношениях. И, наконец, всеобщей безопасности не может быть без **обеспечения стабильного и справедливого международного климата** во всех областях сотрудничества (экономике, финансах, торговле, экологии и др.).

Представляется, что, опираясь на этот багаж, мировому сообществу следует принять **универсальные правила предотвращения военных конфликтов,** которые могут возникать

---

1 **Резолюция Генеральной Ассамблеи ООН от 4 декабря 1986 г. №41/92 «О создании всеобъемлющей системы международного мира и безопасности»; Резолюция Генеральной ассамблеи ООН от 7 декабря 1987 г. № 42/93 «Всеобъемлющая система международного мира и безопасности»; Резолюция Генеральной ассамблеи ООН от 7 декабря 1988 г. № 43/89 «Всеобъемлющий подход к укреплению международного мира и безопасности в соответствии с Уставом Организации Объединенных Наций».**

вследствие враждебного использования информации и ИКТ. Кроме того, необходимо установить **международную ответственность** за нарушение этих правил и незыблемо их соблюдать.

Ни одно должностное лицо органов государственной власти всех стран мира не должно распространять с использованием ИКТ непроверенную, а тем более лживую информацию, которая затрагивает национальную гордость других народов, а также честь и достоинство руководства зарубежных государств, подрывает уважение к государственному суверенитету, позволяет влиять на внутренние дела других государств. За эти деяния должна быть предусмотрена строгая международная ответственность, а руководство суверенных государств обязано твердо следовать этим правилам. Такая же ответственность должна налагаться и на тех, кто использует ИКТ для трансграничного воздействия на критически важные инфраструктуры и другие социально-значимые информационные объекты.

В отношении возможных правил предотвращения военных конфликтов, которые могут возникнуть в результате враждебного использования информации и ИКТ, на наш взгляд, должны выполняться определенные требования.

Во-первых, до принятия правил необходимо выработать единый общепризнанный международный словарь терминов и определений в области их юрисдикции. К таким терминам, ждущим своего определения, например, относятся «информационный инцидент», «информационное нападение», «информационная война» и др. Полагаем, что в международном праве, регулирующем вопросы войны и мира в информационной сфере, каждый термин должен быть понятен, прозрачен, иметь единообразное понимание и единообразно понимаемые критерии.

Во-вторых, новые правила должны иметь одинаковую юридическую силу с нормами и принципами существующего

международного права, регулирующего вопросы войны и мира. Недопустимо, чтобы какому-нибудь юному хакеру на основе косвенных улик правоохранительные органы соседнего государства

вменяли совершение преступления против мира и безопасности человечества за то, что он по своей глупости заблокировал работу органов государственного управления в этой стране. И в это же время глава государства, по указанию которого осуществляется массированная компьютерная атака на коммерческие банки соседней державы, не нес за это никакой международной ответственности. Предусмотренные на этот счет американские санкции во исполнение соответствующего указа президента США Б.Обамы[2] не в счет. Российская Федерация не поддерживает санкционную политику в принципе и считает санкции, принятые в обход ООН, противоречащими международному праву.

В-третьих, правила существующего международного права, должны быть адаптированы к специфике информационного пространства. По этому поводу в последнее время бурная дискуссия с нашими западными партнерами во главе с США на всех международных площадках и форумах. Они призывают признать автоматическую применимость норм и принципов международного права к регулированию военного использования информационно-коммуникационных технологий. В первую очередь, по их мнению, это относится к возможности применения военной силы в ответ на трансграничное информационное воздействие, опираясь на положения статьи 51 Устава ООН (о праве на самооборону) и статьи 5 Вашингтонского договора (о коллективном реагировании на агрессию в отношении какого-члена НАТО).

Российская позиция состоит в том, что, не отрицая незыблемость права на самооборону, необходимо провести большую работу по созданию международно-правовой базы, с использованием которой

2 **Executive Order: «Blocking the property of certain persons engaging in significant malicious cyber-enabled activities)). The White House. April 1,2015.**

можно будет адекватно осуществлять его реализацию применительно к специфике информационной сферы. В ее состав должны войти:

универсальные критерии отнесения различного типа информационных воздействий к актам агрессии (вооруженного нападения);

методология организационно-правового и технологического характера, предназначенная для регламентации процессов выявления и достоверной идентификации источников информационных воздействий;

процессуальные нормы, регламентирующие порядок расследования фактов проведения информационных воздействий, включая методику сбора доказательной базы, позволяющей предъявить обвинение виновным лицам в осуществлении акта агрессии с использованием ИКТ.

Убеждены, что первым шагом на пути формирования правил предотвращения военных конфликтов, которые могут возникнуть в результате враждебного использования информации и ИКТ являются «Правила поведения государств в области международной информационной безопасности», разработанные государствами -членами Шанхайской организации сотрудничества и вынесенные на рассмотрение 69 сессии Генеральной Ассамблеи ООН[6].

Они развивают и дополняют концепцию всеобъемлющей международной безопасности применительно к информационной сфере и создают хороший задел для последующего формирования всеобщей системы международной информационной безопасности.

Ее основу могут составить региональные системы международной безопасности, создаваемые на пространстве Содружества Независимых Государств, Организации Договора о коллективной безопасности и Шанхайской организации сотрудничества[7].

Полагаем, что эти международные форматы, в силу их привлекательности для развивающихся стран и равноправной основы сотрудничества, будут выступать гарантами мира,

' Документ ООН А/69/723.

[7] Современное состояние и перспективы развития военного сотрудничества Российской Федерации в области международной информационной безопасности // под общей редакцией Комова С.А. М.: Министерство обороны Российской Федерации, 2014.

основанного на твердом соблюдении правил предотвращения военных конфликтов, развивающих общепризнанные принципы международного права применительно к специфике глобального информационного пространства.

Мы призываем наших западных коллег внимательно рассмотреть наши предложения и присоединиться к ним.

Благодарю за внимание!