

Confidential

RUSSIA

The circulation of this report has been strictly limited to the members of
the Trialogue Club International
and of the Centre russe d'études politiques.

This issue is for your personal use only.

Published monthly in Russian and in English
by Trialogue Company Ltd.

Issue № 5 (245), vol.16. 2017

26 июня 2017 г.

Редакция *Russia Confidential* сообщает из Москвы:

МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ СЕГОДНЯ: ВМЕСТЕ С РОССИЕЙ, БЕЗ РОССИИ ИЛИ ПРОТИВ НЕЕ?

*(по итогам VI Московской конференции по международной безопасности,
организованной Министерством обороны Российской Федерации)*

(ПРОДОЛЖЕНИЕ; НАЧАЛО В №4 (244))

АННОТАЦИЯ

*В этом номере *Russia Confidential* мы продолжаем фиксировать ключевые моменты выступлений недавно состоявшейся в Москве VI Московской конференции по международной безопасности, собравшей ведущих экспертов, военных специалистов и практиков в области безопасности из 86 стран мира.*

Темами этого номера стали информационная безопасность - впервые за историю Московской конференции вынесенная в отдельную дискуссию - и проблематика ПРО. Показательно, что дискуссия на тему противоракетной обороны прошла в новом формате совместного брифинга, став примером практического сотрудничества российского и китайского оборонных ведомств.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ:
ПРОСТРАНСТВО РАВНЫХ ПРАВ ИЛИ АРЕНА БОРЬБЫ ЗА ПРЕВОСХОДСТВО?

Тема информационной безопасности была вынесена в отдельную дискуссию впервые за историю Московской конференции, тем самым подчеркнув особую актуальность темы.

Секретарь Совета Безопасности России Николай Патрушев подчеркнул такие проблемы в области информационной безопасности, как подтасовка и фальсификация данных с целью вмешательства внешних сил во внутренние дела, а также стремление сохранить односторонние преимущества в управлении глобальной информационной инфраструктурой, в противовес усилиям по созданию системы международной информационной безопасности под эгидой ООН. Если НАТО стремится к обеспечению кибербезопасности только для членов Альянса, то Россия выступает за равную безопасность для всех государств.

Начальник Генштаба ВС России Валерий Герасимов указал на решение НАТО о возможности задействования статьи 5 о коллективной обороне Вашингтонского договора в ответ на кибератаку.

- *Поскольку идентифицировать истинные источники подобных атак сегодня практически невозможно, такая политика Альянса может привести к бездоказательному назначению виновных и применению к ним силы, предостерег В.В. Герасимов.*

Подробно о подходах российских военных рассказал ключевой российский эксперт по теме информационной безопасности, **заместитель начальника Главного оперативного управления Генштаба ВС России Игорь Дылевский**. Он подчеркнул, что информационные технологии все чаще используются в агрессивных целях и даже способны спровоцировать развязывание межгосударственного военного конфликта, что показывают примеры цветных революций и конфликтов последнего десятилетия. Эксперт отметил тот факт, что сегодня очень многие страны (по некоторым оценкам, более 120) разрабатывают информационное оружие – технологии, средства и методы, специально предназначенные для целей ведения информационной войны и потенциально способные нанести огромный ущерб.

- *В России, заметил И.Н. Дылевский, понимают, что запретить разработку такого оружия или проконтролировать его наличие у государств, а тем более террористов не удастся. В то же время Россия считает возможным выработку механизмов нераспространения информационного оружия и снижение вероятности его применения против объектов критической инфраструктуры государств.*
- *Другого подхода, по мнению российского военного, придерживаются на Западе. Решения НАТО последних лет предусматривают возможность применения военной силы для коллективной обороны в ответ на кибератаку, а также признают киберпространство новой операционной средой для коллективной обороны.*
- *С российской точки зрения, деструктивное воздействие на объекты информационной сферы страны может быть квалифицировано как нарушение суверенитета и приравнено к актам агрессии. Но для этого перечень актов агрессии, утвержденный Генеральной Ассамблеей ООН в 1974 г., должен быть дополнен. Россия считает, что в вопросе возможности использования права государств на самооборону и коллективную оборону (статья 51 Устава ООН) в ответ на нападение с использованием информационного оружия нет полной ясности. В отсутствии соответствующего международно-правового документа квалифицировать информационную атаку как вооруженное нападение может СБ ООН, и в таком случае у пострадавшей стороны будет право на самооборону.*
- *В части применимости гуманитарного права к информационным атакам и войнам для России очевидно, что ряд традиционных критериев определения статуса комбатанта не может быть применим к лицам, действующим в информационном пространстве, поэтому требуется разработка и внедрение новой международно-правовой методологии.*

Заместитель Председателя Государственной Думы Российской Федерации Ирина Яровая сделала краткий экскурс в эволюцию американского подхода сначала к психологической, а сегодня к информационной войне.

- *Одна из черт этого подхода, по словам депутата, – ведение информационной войны уже в мирное время. Исходя из этого, информационные нападки со стороны США можно считать прологом к дальнейшим враждебным действиям. В разных странах мира, в частности, в ходе «арабской весны», используется одна и та же технология: сначала осуществляется информационная интервенция, а вслед за ней следует экономическая и политическая колонизация страны.*
- *США фактически монополизировали и приватизировали информационное пространство. Так, американская корпорация ICANN обладает исключительным правом присвоения доменов и тем самым выступает единственным сувереном в мире, способным разрешать или запрещать находиться кому-либо в информационном пространстве.*
- *Показательно различие толкования информационного пространства в доктринальных документах России и США: в то время как российская военная доктрина говорит о нем как о пространстве безопасности, равных и суверенных прав, США делают акцент на стремлении обеспечить собственное информационное превосходство.*

Президент группы компаний InfoWatch Наталья Касперская напомнила о недавно опубликованном *WikiLeaks* массиве предположительно внутренних документов ЦРУ, из которого стало известно о существовании в этой организации отдельного подразделения, занимающегося маскировкой вирусов под желаемые разработки других стран, среди которых назывались Россия, Китай и арабские страны. Н.И. Касперская подчеркнула, что в свете раскрытия этого факта любые попытки приравнять кибератаку к конвенциональной атаке становятся чрезвычайно опасными, поскольку возрастает риск того, что жертва атаки нанесет ответный удар по объектам не причастной к инциденту стороны.

Израильский эксперт Яков Кедми подчеркнул, что, как и любые военные действия, информационные войны всегда преследуют политические цели. В отличие от военных операций, информационная война ведется и до начала, и во время, и после окончания военных действий. Успешная информационная война всегда наступательна – попытки вести ее оборонительно почти всегда заканчиваются поражением. Поскольку работа любых СМИ возле поля боя отличается качеством безответственности, они должны находиться под контролем, чтобы их деятельность не нанесла ущерб операции и войскам. Все донесения с поля боя должны проходить военную цензуру, иначе они должны считаться нарушением закона. Такие и более жесткие меры применяют и демократические страны.

Журналист, член Общественного совета при Министерстве обороны России Владимир Соловьев отметил, что ко внешним угрозам в информационном пространстве нужно относиться как к данности, понимая, что полностью устранить их невозможно. Нужно решать внутренние задачи страны, опираясь на стройную и мощную идеологическую платформу, закрепленную государством и выполняющую функцию иммунитета общества.

Старший советник Атлантического совета Харлан Уллман подчеркнул важность диалога между США и Россией по вопросам использования киберпространства для лучшего понимания подходов и намерений друг друга. Этим могут заниматься госорганы или компании – представители отрасли из обеих стран, но в любом случае коммуникация должна начаться безотлагательно. В противном случае политические разногласия по этим вопросам будут только усугубляться, в чем не заинтересованы ни одна сторона.

Профессор Центра информационной безопасности Академии национальной обороны Народно-освободительной армии Китая (НОАК) Вэнь Байхуа рассказал, что в Китае баланс между безопасностью информационного пространства и свободой доступа к информации соблюдается благодаря принципу кибер-суверенитета, утверждающего право каждой страны управлять

киберпространством так, как она считает нужным, не допуская вмешательства со стороны других государств. Этот принцип продвигался Китаем и Россией в докладе Группы правительственных экспертов ООН 2015 г. и был повторно подтвержден лидерами двух стран в том же году. В долгосрочной перспективе основным способом решения проблем, по мнению Вэнь Байхуа, должно стать международное сотрудничество в киберпространстве в различных областях: этот путь менее затратный, более устойчивый и эффективный.

ПРО: О ВЗГЛЯДАХ РОССИИ И КИТАЯ И ЭВОЛЮЦИИ АРГУМЕНТОВ США

На конференции впервые состоялся совместный российско-китайский брифинг, посвященный противоракетной обороне и ее влиянию на региональную и международную безопасность.

В ходе брифинга **первый заместитель начальника Главного оперативного управления Генштаба ВС России Виктор Познихир** пояснил, чем вызваны озабоченности России (а также и Китая) в отношении развертывания глобальной противоракетной обороны США, представив подробную оценку потенциала американской ПРО в обозримой перспективе:

- *Информационные возможности американской ПРО, обеспечиваемые стационарными и мобильными РЛС и космическими средствами, позволяют не только обнаруживать старты межконтинентальных баллистических ракет (МБР) России и сопровождать их на траектории полета, но и выдавать целеуказания для перехвата.*
- *В.В. Познихир привел оценку, согласно которой к 2022 г. количество противоракет системы ПРО США составит более 1000 единиц, а в перспективе превысит число боевых блоков, развернутых на российских МБР.*
- *Более того, в результате ведущейся модернизации противоракет, они будут способны поражать российские и китайские МБР не только на среднем и конечном, но и на восходящем участке траектории полета.*
- *На кораблях ПРО и на базах ПРО в Румынии и Польше (планируемых к введению в строй в 2018 г.) используются универсальные пусковые установки, в которых могут размещаться как противоракеты, так и крылатые ракеты "Томахок" с дальностью стрельбы до 2500 км.*

Эти выводы В.В. Познихир проиллюстрировал результатами компьютерного моделирования сценариев перехвата российских и китайских МБР средствами американской системы ПРО, подготовленного научно-исследовательскими учреждениями Минобороны России.

Таким образом, ударный потенциал систем ПРО повышает неопределенность и представляет угрозу для безопасности России и Китая, а в случае развертывания наземных пусковых установок является нарушением Договора о РСМД. При этом все российские инициативы по разрешению проблемы ПРО были отвергнуты США, что вынуждает Россию принимать адекватные ответные меры. На вопрос участника из зала о том, какие действия американцев и их европейских союзников могли бы снять опасения России, В.В. Познихир ответил, что главное, что необходимо, – это реальное желание США вести диалог по противоракетной тематике с учетом российских, а также китайских интересов.

В свою очередь, китайский коллега, **заместитель начальника Главного оперативного управления Объединенного штаба Центрального военного совета КНР Цай Цзюнь** заметил, что одностороннее развитие глобальной системы ПРО при игнорировании вопросов общей безопасности и законных прав других стран выглядит как стремление к абсолютному одностороннему военному превосходству – а это может закрепить опасную тенденцию решения международных проблем силовыми методами, привести к гонке вооружений, усугубить напряженность на региональном уровне.

Цай Цзюнь сосредоточил внимание на ситуации на Корейском полуострове и сделал вывод, что размещение Соединенными Штатами системы ПРО в АТР неизбежно стимулирует

КНДР к усилению своего ядерного и ракетного потенциалов. При развертывании ПРО создаются условия для силового решения вопросов на полуострове США и Республикой Корея. Однако практика последних лет показала, что стратегия угрозы силой не работает. Поэтому шаги США и союзников по созданию кольца окружения ПРО в АТР лишь усугубляют их противостояние с КНДР, повышая опасность обострения ситуации на полуострове и идя вразрез с усилиями мирового сообществ решить проблему политическими средствами.

Цай Цзюнь опроверг заверения США и Республики Корея о том, что размещение системы ТНAAD предназначено исключительно для защиты от ракетной угрозы со стороны КНДР.

➤ **С дальностью РЛС комплекса ТНAAD более 2000 км можно отслеживать не только ракеты, запущенные с Корейского полуострова, но и испытательные полеты ракет наземного и морского базирования в северо-восточном районе и районе залива Бохайвань Китая. Очевидно, что настоящая цель размещения системы ТНAAD – создать дополнительный элемент глобальной ПРО США, чтобы в дальнейшем нарастить потенциал азиатско-тихоокеанского сегмента ПРО против Китая и России.**

Цай Цзюнь напомнил о подписанном в июне 2016 г. совместном заявлении лидеров Китая и России об укреплении глобальной стратегической стабильности, в котором обе страны выступили против размещения систем ПРО в Европе и Азии внерегиональными силами, и заявил, что Китай и Россия будут предпринимать дальнейшие ответные меры для обеспечения своих интересов в сфере безопасности и стратегической стабильности.

После брифингов с российской и китайской стороны в рамках дискуссии выступил представитель научного учреждения, занимавшегося представленным моделированием, **начальник Центрального научно-исследовательского института Войск воздушно-космической обороны Министерства обороны РФ Сергей Ягольников**. Он отметил, что несмотря на заявления американской стороны о невозможности перехвата МБР России противоракетами, расчеты российских специалистов показывают иную картину.

➤ **Наличие информации о местах базирования российских МБР и использование данных космических средств позволяет осуществлять пуск противоракет за существенно более короткое время после старта МБР, чем заявляют США. Это обеспечивает достаточный баланс времени для обстрела российских МБР на восходящем участке их полета.**

С.В. Ягольников отметил, что реализация алгоритма, аналогичного тому, который он представил, была выполнена в ходе совместных учений России и НАТО в 2012 г. на модели немецкой компании IABG. Тогда ни у руководителя американской делегации, ни у руководителя делегации НАТО не возникло сомнений в возможности такого перехвата. К таким же выводам пришли ряд американских ученых.

Директор Центра военно-политического анализа Гудзоновского института Ричард Вайтц признал, что ПРО в Европе остается яблоком раздора между США и другими странами, прежде всего Россией. Хотя США, Россия и Китай заинтересованы в прогрессе в сфере сокращения вооружений, все три страны проводят модернизацию своих ядерных сил, так что взаимодействие по этому вопросу затруднено даже независимо от разногласий по противоракетной обороне. В то же время администрация Дональда Трампа пытается доказать России и Китаю, что Иран остается ядерной угрозой, а сделка по поводу иранской ядерной программы – это временная мера. Касательно региональной системы ПРО в Республике Корея Р. Вайтц предположил, что стороны могли бы рассмотреть ряд мер для обеспечения того, чтобы система сдерживала только северокорейскую ядерную угрозу, например, вариант создания многонациональной сети ПРО, аналогичной той, которую НАТО и Россия обсуждали в Европе. Международное сотрудничество по ПРО в контексте ситуации на Корейском полуострове способствовало бы безопасности в регионе и в дальнейшем могло бы охватить и вопросы разоружения.

Модератор дискуссии, **председатель Совета ПИР-Центра генерал-лейтенант запаса Евгений Бужинский** заметил, что, с российской точки зрения доводы о том, что США разворачивают столь большую группировку ПРО для перехвата не существующей на сегодняшний день иранской ракеты, искусственны и не выдерживают критики – учитывая и то, что Иран не планирует создание ракеты с дальностью более 2400 км, не говоря уже о межконтинентальной баллистической ракете.

Е.П. Бужинский также напомнил, что прежде США аргументировали размещение элементов системы ПРО в Польше и Чехии необходимостью перехвата иранских и северокорейских ракет в случае попыток нанести удар по территории США. Однако российские военные обратили внимание американцев на расстояние до США, которое северокорейские ракеты должны будут преодолеть при их запуске через территорию России – и КНДР выпала из аргументации в части ПРО в Европе.

Эксперт сделал и более дальний экскурс в историю, напомнив об изначальной американской аргументации в пользу необходимости заключения Договора по ПРО 1972 года. Бывший в то время министром обороны Р. Макнамара убедил советское руководство в том, что система ПРО – отнюдь не оборонительная система, ибо предназначена для отражения ответного удара и минимизации ущерба от него и фактически является оружием потенциального агрессора и дестабилизирующим элементом стратегической стабильности.

Подобная эволюция аргументов показывает исключительную гибкость США в привлечении и отбрасывании доводов, исходя из собственных национальных интересов на текущий момент.

ВМЕСТО ЗАКЛЮЧЕНИЯ

В работе VI Московской конференции по безопасности приняли участие более 800 гостей из 86 стран. В Москву прибыли 56 официальных военных делегаций. 22 из них возглавили лично руководители оборонных ведомств. Среди участников было более 200 иностранных и российских представителей экспертного сообщества и неправительственных организаций, а также 7 международных организаций. На конференции было аккредитовано более 300 журналистов, представлявших более 80 средств массовой информации со всего мира.

О весомом переговорном потенциале площадки MCIS говорит уже тот факт, что форум собрал за одним круглым столом таких, казалось бы, непримиримых соперников, как Индия и Пакистан, а также одновременно представителей Израиля, Ирана и Сирии.

Но нельзя не сказать и о том, кого на этом представительном форуме не было. Ни НАТО, ни США, с которыми было бы особенно важно наладить диалог в борьбе против терроризма, своих официальных представителей на конференцию не прислали. Таким образом, несмотря на общее понимание, что для эффективной борьбы с терроризмом необходима консолидация мировых усилий, самой большой проблемой остается достижение согласия сторон, которые участвуют или должны участвовать в этой борьбе.

Нежелание Запада вести серьезный диалог с Россией ставит под вопрос не только чаяния мирового сообщества о формировании широкого антитеррористического фронта, но и об улучшении ситуации по другим направлениям международной безопасности, обсуждавшимся на VI Московской конференции. Стоит ли пытаться строить международную безопасность без участия России или, тем более, вооружаясь против нее? Конференция дала на это однозначный ответ – нет.

(с) Международный клуб Триалог: trialogue@pircenter.org;
(с) Centre russe d'études politiques: crep@pircenter.org
Москва-Женева, Май 2017 г.

Выдержки из документа «Международный Клуб Триалог. Условия и правила членства».

3. Права членов Клуба

3.1. Индивидуальные члены Клуба имеют право:

3.1.3. Получать 1 экземпляр бюллетеня эксклюзивной аналитики *Russia Confidential* по электронной почте, на выбранном языке (русском или английском). По правилам Клуба, передача бюллетеня третьим лицам не допускается.[...]

3.2. Корпоративные члены Клуба имеют право:

3.2.3. Получать 2 экземпляра бюллетеня эксклюзивной аналитики *Russia Confidential* по электронной почте, на выбранном языке (русском или английском) либо на обоих языках одновременно, передавать этот бюллетень другим представителям корпоративного члена Клуба. По правилам Клуба, передача бюллетеня третьим лицам, не являющимся членами Клуба, не допускается.[...]

4. Обязанности членов Клуба

4.1. Все срочные члены Клуба обязаны:

4.1.6. Не передавать полученные материалы бюллетеня *Russia Confidential*, а также пароли доступа на сайт Клуба физическим и юридическим лицам, не являющимся членами Клуба. [...]

6. *Russia Confidential*

6.1. Бюллетень эксклюзивной аналитики *Russia Confidential* выпускается ООО «Триалог» исключительно для личного пользования членов Клуба.

6.2. Бюллетень содержит сжатую эксклюзивную аналитику по вопросам международной безопасности, внешней и внутренней политики России и государств СНГ, подготовленную ведущими экспертами специально для *Russia Confidential*.

6.3. В течение не менее 30 дней со дня выхода материалы бюллетеня являются конфиденциальными и не могут цитироваться и передаваться лицам, не являющимся членами Клуба.

6.4. По прошествии не менее чем 30 дней ООО «Триалог» может снять эксклюзивный и конфиденциальный статус с материала, после чего в этих случаях он может быть опубликован в других изданиях и может быть использован для цитирования членами Клуба.

6.5. Бюллетень распространяется по электронным адресам членов Клуба 1 раз в месяц по русскому или английскому языку, по выбору члена Клуба.

6.6. По запросу члена Клуба, он может также получить бумажную версию бюллетеня на выбранном им языке.

Уважаемые члены Международного клуба Триалог,

Продолжается сезон-2017 работы Клуба, и мы рады **пригласить Вас продлить членство в Международном клубе Триалог на 2017 год или на 2017 - 2018 годы.**

В 2017 г. члены Клуба продолжают получать от нас эксклюзивную информацию по вопросам, связанным с приоритетами внешней политики Российской Федерации, а также современными вызовами и угрозами международной безопасности. На 2017 г. запланировано проведение **5 заседаний Международного клуба Триалог**, 4 из которых пройдут в Москве, а 1 за рубежом. Члены клуба получают серию статей журнала *Индекс Безопасности в электронном виде*, **12 номеров** бюллетеня эксклюзивной аналитики *Russia Confidential* (на русском или английском языке), наши электронные информационные и аналитические рассылки.

Как и прежде, специалисты Международного клуба *Триалог* и партнерской организации ПИР-Центра открыты к обмену мнениями по ключевым международным проблемам.

Членство в клубе с 2017 г.

Период	Индивидуальное	Корпоративное
01.01.17 – 31.12.17 (1 год)	50 000 руб.	80 000 руб.
01.01.17 – 31.12.18 (2 года)	90 000 руб.	140 000 руб.

Напоминаем Вам, что в рамках **корпоративного** членства действует **схема «1+1»**, когда в работе Клуба участвуют **два представителя** одной организации.

По всем вопросам, связанным с членством в Международном клубе *Триалог*, следует обращаться по электронной почте secretary@trialogue-club.ru или по тел.: +7 (985) 764-98-96.

С уважением,

**Председатель,
Международный клуб
Триалог**

Е.П. Бужинский