
КРУГЛЫЙ СТОЛ

# ВОЗМОЖНЫЕ ГУМАНИТАРНЫЕ ПОСЛЕДСТВИЯ КИБЕРВОЙН

**11 СЕНТЯБРЯ 2018**

**ИНСТИТУТ ОБОРОННЫХ ИССЛЕДОВАНИЙ И АНАЛИЗА, НЬЮ-ДЕЛИ**

ОРГАНИЗОВАНО СОВМЕСТНО
ИНСТИТУТОМ ОБОРОННЫХ ИССЛЕДОВАНИЙ И АНАЛИЗА (IDSA)
МЕЖДУНАРОДНЫМ КОМИТЕТОМ КРАСНОГО КРЕСТА (МККК)

idsa | ICRC

ОТЧЕТ


## ПРИВЕТСТВЕННОЕ СЛОВО

## Ив Хеллер

**Заместитель главы региональной делегации МККК**

Открывая заседание круглого стола, Ив Хеллер поблагодарил Институт оборонных исследований и анализа (IDSA) за предоставление площадки для обсуждения вопросов современных технологий и современной войны. Назвав МККК хранителем международного гуманитарного права (МГП), он сказал, что МГП рассматривает такие современные проблемы, как автономные системы вооружений (АСВ), кибервойны и ядерное оружие, и их взаимосвязь с принципами МГП, особенно нормами о соразмерности и мерах предосторожности. Приведя примеры программных атак на оборудование и службы, он отметил, что до сегодняшнего дня кибератаки не применялись в контексте вооруженных конфликтов. Однако он добавил, что Индия находится на третьем месте по числу киберугроз и на втором – по числу целенаправленных кибератак. Он подчеркнул, что если критическая инфраструктура Государств подвергнется кибератакам, гражданское население может лишиться питьевой воды, электричества, медицинской помощи, образовательных услуг и продуктов питания. В результате атак на системы GPS могут возрасти жертвы среди гражданского населения, могут также быть затронуты объекты, управляемые компьютерными системами, такие как плотины и атомные электростанции.

МККК заинтересован в том, чтобы МГП применялось к кибероперациям, что позволит предотвратить или ограничить потенциальный ущерб и гуманитарные последствия. МККК призывает государственные вооруженные силы и негосударственные вооруженные группы действовать в соответствии с международным правом, включая МГП, прибегая к кибероперациям. Он заверил, что МККК будет и дальше развивать свои компетенции в области МГП и мер защиты гражданского населения, чтобы противостоять этим вызовам. Хотя киберпространство представляет собой неизведанную территорию, необходимо понимать возможные гуманитарные последствия, как в случае АСВ. Он поставил следующие вопросы:

1. Учитывая взаимосвязанность киберпространства, какие структуры могут быть сформированы для защиты критической гражданской инфраструктуры?
2. Распространяется ли на плотины и атомные электростанции та же защита по МГП в киберпространстве?
3. Какие меры могут принять Государства, чтобы защитить гражданское население и гражданские объекты от враждебных действий в киберпространстве?

Он отметил, что во времена, когда возникают гуманитарные потребности, а законы систематически нарушаются, технологические новшества становятся важнейшим компонентом реагирования, и нельзя допустить, чтобы кибервойны помешали этому. Он вновь подчеркнул крайнюю необходимость обмена информацией в такой значимой стране, как Индия, где имеется аудитория экспертов.


## ВСТУПИТЕЛЬНОЕ СЛОВО ПРЕДСЕДАТЕЛЯ

## Алок Деб, генерал-майор в отставке

**Заместитель генерального директора IDSA**

Генерал-майор Деб поприветствовал участников и отметил, что IDSA и МККК связывают узы плодотворного сотрудничества. Он особо отметил, что специалистам в области безопасности необходимо понимать специфику новшеств в сфере кибервойн, чтобы работать в соответствии с МГП. Обращаясь к теме обсуждения, он подчеркнул, что киберпространство влияет на все аспекты гражданских и военных операций. Он поднял вопрос о разграничении военной и гражданской сфер с учетом их взаимосвязанности. Цитируя «Таллиннское руководство» НАТО, он заявил, что наступательные или оборонительные кибероперации, которые, как следует ожидать, приведут к ранениям и гибели людей, повреждению или разрушению объекта, также можно рассматривать как вооруженный конфликт. Он пояснил, что киберконфликт можно трактовать двояко: киберконфликт как прямой акт войны и киберконфликт, почти равнозначный военным действиям. По мере развития новых технологий, включая блокчейн, ИИ и машинное обучение, сфера ведения кибервойн также будет расширяться.


# КИБЕРОПЕРАЦИИ, КИБЕРАТАКИ И КИБЕРВОЙНЫ: ЗНАЧЕНИЕ И МАСШТАБЫ

## Умеш Кадам

**Консультант МККК**

Умеш Кадам начал с пояснения ключевой терминологии в области МГП, которая может применяться к киберконфликтам. Он отметил, что не существует какого-либо обязательного к применению международного правового документа, касающегося кибервойн, и что в настоящее время решения принимаются в рамках оборонных форумов, гуманитарных организаций и ООН. Он сообщил, что будет опираться на «Таллинское руководство», которое определяет кибероперации как «развертывание киберпотенциала для достижения целей в киберпространстве», а киберпространство – как «среду, образованную физическими и нефизическими компонентами для хранения, модификации и обмена данными с использованием компьютерных сетей». Там же упоминается кибератака как «любая наступательная или оборонительная операция, которая, как следует ожидать, приведет к ранениям и гибели людей, повреждению или разрушению объектов». То есть, кибероперации, приводящие к ранению или смерти, повреждению или разрушению, являются кибератаками. Докладчик пояснил, что МГП применяется только тогда, когда кибератаки имеют место в контексте вооруженного конфликта. С другой стороны, кибервойна – это любая враждебная мера в отношении любого «противника» с целью обнаружения, уничтожения, нарушения целостности, перемещения или сохранения данных посредством компьютера. Традиционно в случае столкновения вооруженных сил двух или более государств такое столкновение квалифицируется как международный вооруженный конфликт (МВК). Однако в контексте кибероперации такая трактовка оспаривается.

Он пояснил, что, если кибероперации проводятся в ходе уже протекающего МВК, такие операции регулируются в рамках МГП. Часто поднимается вопрос о том, могут ли кибероперации как таковые приводить к МВК. Также возможно, что кибероперации сами по себе приводят к МВК, регулируемым в рамках МГП, и что может иметь место немеждународный вооруженный киберконфликт, также регулируемый МГП. Он привел пример проведения Великобританией кибероперации против ИГИЛ на фоне текущего немеждународного вооруженного конфликта (НМВК). Наконец, кибероперации могут проводиться вне контекста вооруженного конфликта, когда МГП не применяется. Такие случаи регулируются правом в области прав человека, законами, касающимися ответственности Государств, мер противодействия и обязательства Государств проявлять должную осмотрительность. Докладчик признал, что гуманитарные последствия кибероперации вне рамок вооруженного конфликта также возможны. По его словам, эксперты согласны в том, что нужны дополнительные правовые нормы, так как действующие нормы гуманитарного права не охватывают всего, что происходит в контексте кибероперации.

### КОММЕНТАРИЙ ПРЕДСЕДАТЕЛЯ

Председатель подытожил, сказав, что лишь те кибероперации, которые прямо или косвенно приводят к гибели или ранению людей, могут считаться вооруженным конфликтом, и в этом случае применяется МГП. В заключении он сказал, что предстоит проделать большую работу, чтобы стороны во всем мире могли приходить к взаимоприемлемым условиям.


# ЗАЩИТА ОТ ГУМАНИТАРНЫХ ПОСЛЕДСТВИЙ ВОЙНЫ, ПРЕДУСМОТРЕННАЯ В МГП

## Суприйя Рао

**Юридический консультант МККК**

Суприйя Рао заявила, что ее выступление будет касаться договоров по МГП и их роли в регулировании кибервойн. Приведя примеры сообщений СМИ о кибератаках, она отметила, что военный потенциал в киберпространстве находится на этапе формирования и что гуманитарные последствия таких инцидентов можно себе представить, хотя они могут быть и не выражены. Касаясь договорных норм МГП, она пояснила разницу между *jus ad bellum* и *jus in bello*, подчеркнув, что цель МГП – свести к минимуму страдания людей, предоставляя защиту тем, кто не принимает или прекратил принимать участие в военных действиях, и ограничивая выбор средств и способов ведения войны. Хотя в МГП не упоминаются кибервойны, оно все же применимо к ним. Правовая основа для этого заложена в Консультативном заключении Международного Суда по делу о

ядерном оружии, в соответствии с которым, действующие нормы с которым действующие нормы МГП применяются ко всем формам ведения войны, включая будущие, и в статье 36 Дополнительного протокола I (ДП I), в котором предусмотрено обязательство Государств проводить правовую экспертизу видов оружия, которые могут попадать под запрещение согласно МГП.

Рао сослалась на Руководство МККК по правовой экспертизе новых видов оружия в соответствии с обязательством статьи 36. Также она упомянула доклады Группы правительственных экспертов (ГПЭ) ООН 2013 и 2015 гг. по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (в работе ГПЭ Индия также принимала участие). ГПЭ пришла к выводу, что международное право, в частности, Устав ООН, применяется к кибервойнам, наряду с общепризнанными принципами гуманности, необходимости, соразмерности и избирательности. Кроме того, на встрече глав правительств стран Британского Содружества 2018 г. была принята декларация о кибербезопасности, в которой выражено намерение проводить дальнейшие обсуждения о применении МГП к киберпространству.

Говоря об ограничениях, налагаемых на ведение кибервойн согласно МГП, Рао указала, что МГП допускает применение летального оружия, но в то же время решает задачу защиты гражданского населения и гражданских объектов, устанавливая правила избирательности, соразмерности и предосторожности при нападении, известные как правила ведения военных действий. Далее она обратила внимание на некоторые нерешенные вопросы, касающиеся правил ведения военных действий в связи с применением МГП к кибервойнам. Принцип избирательности действует при кибератаках в рамках вооруженного конфликта. Неизбирательное нападение имеет место, когда удар не может быть направлен на определенную военную цель или когда его воздействие не может быть ограничено определенной военной целью. В связи с этим встает вопрос о том, может ли вредоносная программа быть нацелена на определенный военный объект. Несоразмерные нападения определяются как нападения, при которых ожидаемые попутные ранения и потери жизни среди гражданского населения, ущерб гражданским объектам чрезмерны по отношению к прямому военному преимуществу. Это требует военного планирования с прогнозируемыми результатами, которое обеспечит выполнение обязательства о соразмерности. Необходимость применения МГП к кибервойнам вытекает из задачи сохранения критической гражданской инфраструктуры. Такие объекты, как плотины и атомные электростанции, пользуются особой защитой. Нарушение работы медицинских учреждений недопустимо, поэтому кибератака против информационной системы больницы также является нарушением МГП.

Касаясь взаимосвязанности киберпространства и, как следствие, трудностей с применением принципов соразмерности и избирательности, она отметила, что, поскольку существует лишь одно киберпространство, трудно провести различие между военными объектами и гражданской киберинфраструктурой. Во-вторых, трудно заранее оценить сопутствующий ущерб гражданскому населению и гражданским объектам, как того требуют обязательства в рамках МГП в связи с правилами ведения военных действий. В-третьих, определение «нападения» согласно статье 49 ДП I как акта насилия в отношении противника, совершаемого при наступлении или обороне, поднимает вопрос физического ущерба. Можно ли к таковому отнести потерю функциональности? С точки зрения МККК, коль скоро объект был поврежден, не имеет значения, произошло ли это в результате физического воздействия или иным образом. Узкое определение того, что составляет понятие «нападение», не согласуется с объектом и целью МГП – защитой гражданских лиц и объектов от причинения вреда в максимально возможной степени. Наконец, учитывая анонимность, свойственную киберпространству, трудно установить нарушителя, совершившего то или иное действие, а если нарушитель не выявлен, будет трудно сделать вывод о применимости МГП.

## КОММЕНТАРИЙ ПРЕДСЕДАТЕЛЯ

Председатель подчеркнул такие проблемы, как определение соразмерности, рамки кибервойн применительно к информационным операциям, ответственность корпораций по МГП и использование общественного киберпространства в мирное время, что противоречит задаче защиты гражданского населения.


# КИБЕРОПЕРАЦИИ ВО ВРЕМЯ ВООРУЖЕННОГО КОНФЛИКТА: СОВРЕМЕННЫЕ ВОЕННЫЕ ДОКТРИНЫ И БУДУЩЕЕ РАЗВИТИЕ

## Бриг. генерал Ашиш Чхиббар

**Старший научный сотрудник IDSA**

Бригадный генерал Чхиббар начал доклад с описания двух инцидентов с киберпреступлениями. Первый произошел в Северной Корее и поднял такие проблемы, как передача вредоносной программы от системы

к системе, распространение вируса в обход системы защиты без нажатия на ссылку и атаки на определенные системы, не имеющие доменного имени. Более 200000 компьютеров в более чем 150 странах, включая Индию, были выведены из строя, а данные уничтожены. Второй инцидент завершился выплатой выкупа и уничтожением данных глобальной судоходной компании Maersk. Как отметил докладчик, эти случаи заставляют обратить внимание на трудности с атрибуцией кибератак, их каскадный эффект, вопросы взаимодействия транснациональных компаний с разведывательным сообществом и легкость, с которой совершаются атаки. Ссылаясь на Устав Сухопутных войск США, он назвал три категории киберпространства:

1. Физический уровень
2. Логический уровень
3. Социальный уровень (киберперсона)

Он указал, что киберпространство всегда будет благоприятствовать злоумышленнику, так как оно создавалось без учета проблем безопасности. Перечисленные выше три уровня киберпространства могут подвергаться атакам извне. Касаясь вопроса о существующем международном правовом механизме, докладчик заявил, что не следует ожидать правосудия там, где отсутствуют обязательные к исполнению правовые нормы.

Он сравнил доктрины США, Китая и России в области киберпространства. В США использование киберпространства для проведения наступательных операций признано в качестве стратегии. В Китае поставлена задача обеспечить постоянную доступность киберпространства для критической инфраструктуры путем обособления, построить стратегическую сеть для государственной власти и более совершенную систему международного управления киберпространством, которое в настоящее время рассматривается как настроенное в пользу Запада.

Россия, со своей стороны, проявляет интерес к психологическим аспектам киберпространства. В ее доктринах национальной безопасности отражено, что киберпространство используется для манипулирования сознанием граждан.

Далее докладчик заявил, что в киберпространстве 2.0 государственный контроль будет усиливаться, а доступ в Интернет ограничиваться. По его словам, трудно представить себе общий глобальный документ, хотя могут быть заключены двусторонние и многосторонние соглашения. Будут вводиться более строгие меры подотчетности ИКТ-компаний государству, так как они будут становиться объектом контроля в сфере национальной безопасности, и раскрытие информации о сотрудничестве с другими государствами будет обязательным. В заключении докладчик высказал тезис о том, что виды оружия будут неуклонно совершенствоваться, но решение лишить человека жизни не будет отдано искусственному интеллекту.

## КОММЕНТАРИЙ ПРЕДСЕДАТЕЛЯ

Председатель заметил, что, с одной стороны, существует принцип универсального применения норм права, а с другой, существует реальность, в которой действуют государства. По его мнению, обычные люди должны понимать техническую терминологию, так как являются активными пользователями киберпространства.


Участники круглого стола слушают доклад.

Применение МГП к киберпространству необходимо постоянно пересматривать. Он обратил внимание слушателей на вопросы подотчетности и атрибуции и заключил, что страны объединяют усилия во время кризиса, но создание системы превентивных мер остается проблематичным.


## ЭВОЛЮЦИЯ И БУДУЩИЙ ХАРАКТЕР КИБЕРАТАК ПРОТИВ КРИТИЧЕСКИХ СЛУЖБ И ИНФРАСТРУКТУРЫ

### Д-р Манмохан Чатурведи

**Индийский технологический институт (IIT), Дели**

Д-р Чатурведи поднял тему эволюции критической инфраструктуры, вызванной технологическим прогрессом, и ответа Индии на эти процессы. Он пояснил, что критическая инфраструктура (КИ), включающая системы водоснабжения, электроснабжения и т. д., поддерживается критической информационной инфраструктурой (КИИ), которая, в свою очередь, зависит от базовых информационных технологий (ИТ) и систем управления технологическими процессами (СУТП). Статья 70 Закона Индии об ИТ 2008 г. (с изменениями) определяет КИИ как «компьютерные ресурсы, вывод из строя или разрушение которых будет иметь губительные последствия для национальной безопасности, экономики, здравоохранения и индивидуальной безопасности». При чрезмерной защищенности систем возможности их использования ограничены, однако безопасность тоже принципиально важна. В киберпространстве присутствует четыре вида угроз национальной безопасности: кибервойны, кибертерроризм, кибершпионаж и киберпреступность. Появление сетей последующих поколений (NGN) повысило вероятность кибератак и атак на КИ; растет также количество потенциальных точек атаки. Элементы инфраструктуры в значительной мере взаимосвязаны и взаимозависимы, что приводит к каскадному эффекту, который проявляется в условиях стихийных бедствий. Докладчик выделил различные инциденты с недавними атаками на КИ и констатировал, что оценка риска – это срочная необходимость. Система государственного управления должна соответствовать темпам развития технологий, поскольку регулирование критической инфраструктуры крайне важно. На основании Закона об ИТ был создан Национальный центр защиты критической инфраструктуры как ключевое ведомство в системе регулирования Индии, на которое возложен ряд функций, включая определение критических суботраслей, выпуск оповещений, анализ вредоносных программ, киберкриминалистику, просвещение и обучение, техническую поддержку и т. д.

## КОММЕНТАРИЙ ПРЕДСЕДАТЕЛЯ

Председатель обобщил вызов, с которым сталкивается система в Индии, как относящийся не столько к сфере технологии, сколько к сфере управления. После того, как будут приняты в расчет правовые, военные и промышленные аспекты, задача будет сводиться к созданию прозрачной и основанной на принципе равенства системы управления киберпространством.

## СЕССИЯ ВОПРОСОВ И ОТВЕТОВ

Вопросы касались следующих тематических направлений: международный консенсус по проблемам правового регулирования кибервойн, проблема торгового протекционизма, высокоточные системы наведения, применение МГП к негосударственным вооруженным группам, которые ведут кибервойны, и квалификация выведения из строя систем и уничтожения данных как вооруженного конфликта.

По словам Рао, в сфере МГП существуют прежние обязательства, и предполагается, что государства, не являющиеся участниками Женевских конвенций, будут соблюдать обычное международное право. МККК не издает правовые нормы, и реальное уважение к закону должно обеспечиваться на национальном уровне, должно быть частью военной доктрины и практики. Кадам добавил к сказанному, что после некоторого прогресса в 2015 г. ГПЭ испытала спад активности в 2017 г. в связи с тем, что Государствам не удалось достичь единого мнения о применимости МГП в сфере кибернетического права.

На вопрос о высокоточных системах наведения Рао ответила, что трудно предвидеть косвенные последствия атак в киберпространстве, однако защита гражданских объектов и обозначение их как отдельной категории – это давнее обязательство в рамках МГП. Д-р Чатурведи пояснил, что, хотя принцип соразмерности трудно соблюсти, к этой цели стоит стремиться.

Как отметил бригадный генерал Чхиббар, на своем четвертом заседании ГПЭ пришла к выводу, что государства не будут совершать нападения на критическую инфраструктуру других государств, они также не будут нападать на группы экстренного реагирования, ведущие восстановительные работы в киберпространстве, и обязались сотрудничать в случае обнаружения территориальной связи между кибератакой и территорией. По вопросу о негосударственных вооруженных группах Кадам дал пояснение, что МГП будет по-прежнему распространяться на такие преступления, как вербовка детей-солдат, даже если они совершаются в киберпространстве. Государства несут обязательство делать все, чтобы киберпространство не использовалось для причинения вреда другому государству,

согласно принципу ответственности государств, однако приведение в исполнение этой нормы остается проблематичным.

Рао объяснила, что МККК расценивает акт «выведения из строя» как нападение и рассматривает вопрос о том, подпадает ли сам акт выведения из строя, в рамках кибероперации, под действие МГП. В комментарии МККК к общим статьям 2 и 3 сказано, что выведение из строя само по себе не может быть достаточным основанием для достижения порога применения МГП. В случае НМВК должны выполняться оба критерия – интенсивность и организация сторон, и если эти критерии выполняются, такое действие может быть истолковано как вооруженное нападение. Отвечая на вопрос о данных, она сказала, что если уничтожение данных наносит ущерб гражданским объектам, это действие попадает в сферу применения МГП.

## ЗАКЛЮЧИТЕЛЬНОЕ СЛОВО

### Алок Деб, генерал-майор в отставке

**Заместитель генерального директора IDSA**

Генерал-майор Деб сказал, что мы не можем ждать катастрофы, чтобы заняться темой кибервойн. Он признал, что работа МККК трудна, но правительства стран по всему миру предпринимают усилия в этом направлении. Единственное решение заключается в том, чтобы обе стороны встали на единые позиции.

Он подчеркнул, что в дальнейшем следует расширять рамки взаимодействия и привлекать к диалогу граждан всех возрастов.


## ВЫРАЖЕНИЕ БЛАГОДАРНОСТИ

### Саджив Джетли, генерал-майор в отставке

**Глава Департамента МККК по работе с вооруженными силами и органами безопасности**

Генерал-майор Джетли поблагодарил всех присутствующих на круглом столе. Он отметил, что на заседании были подняты важные вопросы, касающиеся кибервойн, и что их обсуждение следует продолжать в рамках подобных форумов. Он выразил признательность Генерал-майору Дебу и его команде в IDSA, докладчикам, участникам и членам МККК за вклад в работу совещания.

Групповое фото: участники круглого стола в полном составе

## О НАС

Международный комитет Красного Креста - независимая неполитическая организация с широким спектром строго гуманитарной деятельности, осуществляемой на основе присутствия в более, чем 80 странах мира. На него возложена общепризнанная обязанность продвигать принципы международного гуманитарного права (МГП) и удовлетворять нужды людей, затронутых гуманитарными проблемами, в особенности в ситуациях вооруженных конфликтов и насилия.

Работая в партнерстве с Национальными обществами Красного Креста и Красного Полумесяца, местными органами власти и другими субъектами, МККК оказывает гуманитарную помощь и дает консультации в таких областях, как международное гуманитарное право, реагирование на чрезвычайные ситуации, услуги медицинской помощи и реабилитации, обеспечение водой и жилищами, помощь в обеспечении средств к существованию, судебная медицина в гуманитарной деятельности, помощь содержащимся под стражей и восстановление семейных связей.

МККК обладает подтвержденным опытом и имеет давнюю историю присутствия в Азии, взаимодействует со всеми заинтересованными сторонами, опираясь на уникальный подход, основанный на конфиденциальном диалоге, прозрачности в осуществлении деятельности, обмене знаниями и партнерстве, чтобы иметь возможность непосредственно работать с уязвимыми группами населения и удовлетворять их нужды.

@ICRC_nd

blogs.icrc.org/new-delhi

**Международный комитет Красного Креста**
Региональная делегация в Индии, Непале, Бутане и Мальдивах
С-6/6, Территория развития Сафдарджунг
Нью Дели - 110016
T: +91 11 42211000 | F: +91 11 42211068
Email: newdelhi@icrc.org | www.icrc.org/in