
Второй день четырнадцатой встречи
MC(14) Journal No. 2, пункт 8 повестки дня

**РЕШЕНИЕ №. 7/06
ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ ИНТЕРНЕТА
В ТЕРРОРИСТИЧЕСКИХ ЦЕЛЯХ**

Совет министров,

напоминая о своем предыдущем решении по этому вопросу (MC.DEC/3/04),

будучи по-прежнему серьезно обеспокоен ростом использования Интернета в террористических целях, как это было отмечено в вышеупомянутом решении и иных документах,

вновь подтверждая в данном контексте важность всестороннего уважения права на свободу мнений и свободу выражения, включая свободу искать, получать и передавать информацию, которые жизненно важны для демократии и фактически укрепляются благодаря сети Интернет (PC.DEC/633 от 11 ноября 2004 года) и верховенству закона,

признавая, что в резолюции 1624 (2005) Совета Безопасности Организации Объединенных Наций содержится призыв к государствам принимать меры, которые необходимы и уместны, и в соответствии с их обязательствами по международному праву законодательно запретить подстрекательство к совершению террористического акта или актов и предотвращать такое поведение,

вновь подтверждая наши обязательства в соответствии с Глобальной контртеррористической стратегией Организации Объединенных Наций, в частности осуществлять "координацию усилий, предпринимаемых на международном и региональном уровнях в целях борьбы с терроризмом во всех его формах и проявлениях в сети Интернет" и "использование сети Интернет в качестве инструмента борьбы с распространением терроризма, признавая при этом, что государствам может потребоваться помощь в этих вопросах",

* Включает поправки, внесенные в результате сверки текста делегациями 29 января 2007 года.

принимая во внимание сделанный в докладе Контртеррористического комитета Организации Объединенных Наций (S/2006/737 от 15 сентября 2006 года) вывод, что ряд государств сообщили о том, что они изучают возможность введения в своем внутреннем законодательстве запрета на подстрекательство применительно к сети Интернет,

отмечая недавно принятые документы, в частности Конвенцию Совета Европы о предупреждении терроризма, в части обязательств государств-участников этой Конвенции ввести уголовную ответственность за публичное подстрекательство к совершению террористического преступления, вербовку и подготовку в целях терроризма,

напоминая о Конвенции Совета Европы по киберпреступности (2001), единственном юридически обязательном многостороннем инструменте, непосредственно посвященном киберпреступности, в частности обеспечивающем общеправовые рамки для международного сотрудничества между государствами-участниками этой Конвенции в борьбе с киберпреступностью, и ее Дополнительном протоколе, касающемся криминализации актов расизма и ксенофобии, совершаемых с помощью компьютерных систем,

признавая обязательство, принятое на Саммите "Группы восьми" (Санкт-Петербург, Российская Федерация, 16 июля 2006 года) об эффективном противодействии попыткам злонамеренного использования киберпространства в целях терроризма, включая подстрекательство к совершению террористических актов, передаче информации и планированию террористических актов, а также вербовку и подготовку террористов, и, в частности, отмечая роль действующей круглосуточно семь дней в неделю Сети "Группы восьми" по борьбе с компьютерными преступлениями для противодействия уголовному поведению в киберпространстве,

напоминая об итогах Специального совещания ОБСЕ по взаимосвязи между расистской, ксенофобской и антисемитской пропагандой в Интернете и преступлениями на почве ненависти (Париж, 15-16 июня 2004 года), а также об итогах Экспертного семинара ОБСЕ по борьбе с использованием Интернета в террористических целях (Вена, 13-14 октября 2005 года) и Экспертного семинара ОБСЕ и Совета Европы по теме "Предупреждение терроризма: борьба с подстрекательством и иной террористической деятельностью" (Вена, 19-20 октября 2006 года), и соответствующей работе, проделанной Секретариатом и институтами ОБСЕ, в частности Представителем по вопросам свободы средств массовой информации и БДИПЧ,

принимая во внимание различные национальные подходы к определению информации "незаконного" и "нежелательного" содержания и различные меры применения незаконной и нежелательной информации в киберпространстве, такие как возможное использование оперативных данных, полученных из переписки и информации в Интернете, для закрытия веб-сайтов террористических организаций и веб-сайтов тех, кто их поддерживает,

будучи обеспокоен продолжающимися атаками хакеров, которые, хотя и не будучи связанными с терроризмом, все-таки демонстрируют наличие экспертных знаний в этой области, и тем самым, обеспечивают возможность террористических кибератак на компьютерные системы, влияющих на функционирование критических инфраструктур, финансовых учреждений или других жизненно важных сетей,

1. Постановляет активизировать деятельность ОБСЕ и ее государств-участников, главным образом путем укрепления международного сотрудничества в деле противодействия использованию Интернета в террористических целях;
2. Призывает государства-участники рассмотреть возможность принятия всех соответствующих мер по защите критической информационной инфраструктуры и информационных сетей от угрозы кибернападения;
3. Призывает государства-участники рассмотреть возможность присоединения в качестве сторон к существующим международным и региональным правовым инструментам, включая конвенции Совета Европы о киберпреступности (2001) и о предупреждении терроризма (2005), и выполнять свои обязательства по этим инструментам;
4. Побуждает государства-участники, в случае необходимости, присоединиться к действующей круглосуточно семь дней в неделю Сети "Группы восьми" по борьбе с компьютерными преступлениями и назначить соответствующий орган/контактное лицо для связи с этой сетью в целях содействия международному сотрудничеству правоохранительных органов в борьбе со злонамеренным уголовным использованием киберпространства и в уголовных делах, в которых используются электронные доказательства;
5. Призывает государства-участники, при получении просьбы о принятии мер в отношении информации, являющейся противоправной по их внутреннему законодательству и размещенной на сайте под их юрисдикцией, принимать все соответствующие меры, направленные против такой информации, и сотрудничать с другими заинтересованными государствами, в соответствии с их внутренним законодательством и принципом верховенства закона, а также согласно их международным обязательствам, в том числе международным стандартам в области прав человека;
6. Предлагает государствам-участникам расширить их мониторинг веб-сайтов террористических/насильственно-экстремистских организаций и их сторонников, а также активизировать обмен информацией в рамках ОБСЕ и других соответствующих форумов по использованию Интернета в террористических целях и мерам противодействия, в соответствии с внутренним законодательством, обеспечивая в то же время соблюдение международных обязательств и стандартов в области прав человека, в том числе касающихся прав на неприкосновенность частной жизни, свободу мнений и свободу выражения, и верховенство закона. Следует избегать дублирования с деятельностью, осуществляемой в рамках других международных форумов;

7. Рекомендует государствам-участникам изучить возможность более активного вовлечения институтов гражданского общества и частного сектора в деятельность по предупреждению и противодействию использованию Интернета в террористических целях;

8. Побуждает государства-участники принять участие в запланированной на май 2007 года "Политической конференции ОБСЕ по партнерству государственного и частного секторов в противодействии терроризму" в Вене, на которой основное внимание будет уделено жизненно важной роли частного сектора, включая деловые круги, гражданское общество и средства массовой информации, которую они могут играть совместно с правительствами в предупреждении терроризма и борьбе с ним;

9. Поручает Генеральному секретарю развивать, главным образом через Контртеррористическую сеть ОБСЕ, обмен информацией об угрозе, возникающей в связи с использованием Интернета в террористических целях, включая подстрекательство, вербовку, сбор средств, подготовку, выбор целей и планирование террористических актов, и информацией о законодательных и иных мерах, принимаемых с целью противодействия этой угрозе.