



**Двенадцатый Конгресс
Организации Объединенных
Наций по предупреждению
преступности и уголовному
правосудию**

Distr.: Limited
14 April 2010
Russian
Original: English

Салвадор, Бразилия, 12-19 апреля 2010 года

Доклад Комитета II: пункт 8 повестки дня и семинар-практикум 2

Добавление

Пункт 8 повестки дня. Последние тенденции в использовании научно-технических достижений правонарушителями и компетентными органами, ведущими борьбу с преступностью, в том числе применительно к киберпреступности

1. На своих 1-3-м заседаниях 12 и 13 апреля 2010 года Комитет II провел общую дискуссию по пункту 8 повестки дня под названием "Последние тенденции в использовании научно-технических достижений правонарушителями и компетентными органами, ведущими борьбу с преступностью, в том числе применительно к киберпреступности". Для рассмотрения этого пункта повестки дня Комитету были представлены следующие документы:

а) подготовленный Секретариатом рабочий документ о последних тенденциях в использовании научно-технических достижений правонарушителями и компетентными органами, ведущими борьбу с преступностью, в том числе применительно к киберпреступности (A/CONF.213/9);

б) Руководство для дискуссий (A/CONF.213/PM.1);

с) доклады региональных подготовительных совещаний к двенадцатому Конгрессу (A/CONF.213/RPM.1/1, A/CONF.213/RPM.2/1, A/CONF.213/RPM.3/1 и A/CONF.213/RPM.4/1).

2. На 1-м заседании 12 апреля с вступительным словом выступил Председатель Комитета. Представитель Секретариата представила рассматриваемый пункт повестки дня. С заявлениями выступили представители Китая, Алжира, Канады, Аргентины, Соединенных Штатов Америки, Саудовской Аравии, Российской Федерации, Германии, Ботсваны, Кубы и Чили. Наблюдатели от Иберо-американской сети оказания правовой помощи (ИберРед), Совета Европы и Всемирного общества виктимологии



также сделали заявления. С заявлением в личном качестве выступил также эксперт из Норвегии.

3. На 2-м заседании 13 апреля с заявлениями выступили представители Испании (от имени Европейского союза), Польши, Республики Корея, Азербайджана, Мексики, Индонезии, Анголы и Аргентины.

4. На 3-м заседании заявления сделали представители Колумбии, Южной Африки, Индии, Перу, Зимбабве, Омана и Бразилии. С заявлением также выступил наблюдатель от Международной ассоциации прокуроров.

Общая дискуссия

5. Открывая дискуссию, Председатель обратил внимание на проблемы, возникающие в связи с киберпреступностью, и отметил способность организованных преступных групп использовать возможности быстро развивающихся технологий в противоправных целях. Он указал на трансграничный характер киберпреступности, нехватку знаний о масштабах этой проблемы и различия в национальных системах.

6. В своем вступительном заявлении представитель Секретариата охарактеризовала киберпреступность как один из серьезнейших вызовов правоохранительной системе и отметила, что государства-члены, представители научных кругов и другие заинтересованные стороны призвали к разработке соответствующей международной конвенции. Государствам необходимо развивать свой потенциал, и в этом деле им могло бы помочь ЮНОДК путем оказания технической экспертной помощи и оперативной поддержки. Одним из эффективных способов наращивания всеобъемлющего и устойчивого потенциала государств в целях пресечения киберпреступности мог бы стать глобальный план действий по наращиванию потенциала с участием ключевых учреждений и партнеров.

7. В ходе дискуссии были признаны многие бесспорные преимущества быстрого развития технологий. Однако в то же время такое развитие позволило новыми способами совершать традиционные виды преступлений, включая мошенничество и распространение материалов, содержащих детскую порнографию, а также породило новые виды преступлений, таких, как хакерство, спамминг, "фишинг" (использование в мошеннических целях поддельных сайтов (или рассылка сообщений со ссылками на такие сайты)), цифровое пиратство, злонамеренное распространение вирусов и другие атаки на критически важную информационную инфраструктуру. Было отмечено, что террористические организации и организованные преступные группы поставили быстрое научно-техническое развитие на службу своей преступной деятельности. Участники дискуссии пришли к единому мнению о том, что киберпреступность представляет угрозу для экономики и жизненно важной инфраструктуры, а также подрывает доверие к институциональным структурам и социально-культурное благополучие.

8. Ораторы обратили внимание на проблемы, возникающие в области борьбы с киберпреступностью. Новые технологии развиваются и становятся широкодоступными настолько быстро, что ни политика, ни законодательство не в состоянии идти с ними в ногу. Наличие различий в правовых системах и недостаточно развитое международное сотрудничество усложняют проведение

расследований киберпреступлений и преследование за их совершение. Сложные технологии вошли в повседневную жизнь, и киберпреступность стала обратной стороной их законного применения. Один из выступавших отметил, что зачастую о киберпреступлениях не заявляют в полицию, поскольку мало верят в их раскрываемость, а в случае, когда мишенями становятся корпорации, причиной являются опасения насчет потери репутации.

9. Различные ораторы сообщили о мерах, принятых правительствами их стран в целях борьбы с киберпреступностью, в том числе об уголовном законодательстве и законах о борьбе с отмыванием денежных средств, регламентировании работы Интернет-кафе, наращивании потенциала, повышении уровня информированности, укреплении механизмов отчетности и защите уязвимых групп. Выступавшие упомянули о создании групп экстренного реагирования, специализированных подразделений и межведомственных платформ для правоохранительного, военного, научного и частного секторов. Ораторы также отметили возможности применения информационных технологий в правоохранительной области, в частности речь шла о системах электронного слежения и наблюдения, искусственном интеллекте и электронных средствах выявления подозрительных финансовых операций и установления IP-адресов. Вместе с тем для расследования киберпреступлений и привлечения к ответственности за их совершение необходимы новые навыки и процессуальные механизмы, в частности возможность сбора и анализа цифровых доказательств и их использования в производстве по уголовным делам. Ораторы подчеркнули важность защиты частной жизни и прав человека в рамках борьбы с киберпреступностью.

10. Многие выступавшие подчеркнули, что успешно бороться с киберпреступностью можно только путем международного сотрудничества. Ряд ораторов призвали государства принять меры по повышению эффективности оказания взаимной правовой помощи и сотрудничества в правоохранительной области. Многие выступавшие сослались на Конвенцию Совета Европы о киберпреступности (Будапештская конвенция) как на наиболее проработанную международно-правовую основу для международного сотрудничества в области борьбы с киберпреступностью. Также упоминались утвержденная в 2007 году Международным союзом электросвязи Глобальная программа кибербезопасности и инициативы Организации американских государств, Группы восьми, Интерпола и Секретариата Содружества. Было отмечено, что в обмене оперативными данными, опытом и извлеченными уроками полезную роль играют сети практических работников. Необходимо укреплять существующие региональные сети и обеспечить их более тесную взаимосвязь.

11. Было признано, что наиболее уязвимыми для киберпреступности являются развивающиеся страны. Развитым странам следует в срочном порядке активизировать деятельность по оказанию помощи в наращивании потенциала, особенно в отношении подготовки сотрудников правоохранительных органов, прокуроров и судей. Частный сектор, в том числе поставщики услуг, должен с полной ответственностью участвовать в этом деле. Был упомянут ряд имеющихся механизмов, включая виртуальный форум для стран Азии, созданный при помощи ЮНОДК, учебный веб-модуль Международной ассоциации прокуроров и подготовленная Международным союзом электросвязи подборка материалов по законодательству в области борьбы с

киберпреступностью. Ораторы сослались на работу ЮНОДК в области борьбы с преступлениями, связанными с использованием личных данных, и рекомендации группы ведущих экспертов по этому вопросу. Ряд выступавших призвали к разработке плана действий по наращиванию потенциала на международном уровне при участии всех заинтересованных международных сторон.

12. Была рассмотрена рекомендация, сформулированная в ходе региональных подготовительных совещаний к двенадцатому Конгрессу, относительно того, что следует тщательно изучить и положительно решить вопрос о разработке глобальной конвенции о борьбе с киберпреступностью. Некоторые ораторы решительно поддержали начало переговоров по новому международному документу, направленному на согласование национальных правовых подходов и налаживание международного сотрудничества. Было высказано утверждение о том, что существующие инициативы носят лишь ограниченный двусторонний или региональный характер. Международный документ, который мог бы стать дополнительным протоколом к Конвенции Организации Объединенных Наций против транснациональной организованной преступности или отдельной конвенцией, развил и дополнил бы положения действующих двусторонних и региональных договоров или соглашений о борьбе с киберпреступностью, включая Будапештскую конвенцию. Один из выступавших предложил вести переговоры относительно нового документа в рамках Комиссии международного права, членом которой могло бы стать ЮНОДК.

13. Другие ораторы высказались против начала переговоров по такому документу. Они сочли Будапештскую конвенцию достаточной рамочной основой, применяющейся в том числе и не подписавшими ее государствами в качестве типового законодательства, позволившего государствам проводить успешные расследования. Было выражено опасение по поводу того, что в глобальном документе, возможно, не удастся установить такие же высокие стандарты и что нынешние усилия по модернизации могут не получить развития во время проведения переговоров по вопросу о разработке нового документа. Проблемы в области борьбы с киберпреступностью были признаны в основном носящими оперативный характер, в свете чего необходимо усовершенствовать механизмы обмена информацией и наращивания потенциала. Было отмечено, что многим странам, которым не хватает экспертного опыта и знаний в области борьбы с киберпреступностью, следует сосредоточиться на решении этих оперативных вопросов, а не на переговорах относительно новой конвенции.

14. Ряд выступавших выразили мнение о том, что сегодня слишком рано приступать к разработке новой конвенции, поскольку прежде необходимо рассмотреть несколько основополагающих вопросов. Некоторые ораторы просили пояснить основную цель и сферу охвата такого нового документа, а один из выступавших рекомендовал провести экспериментальный анализ действующих стандартов. В рамках переговоров относительно новой конвенции пришлось бы решать такие вопросы, как экстерриториальная юрисдикция и сопряженные с этим вопросы национального суверенитета; вопросы, связанные с правами человека, частной жизнью и национальной безопасностью; и необходимость участия частного сектора в процессе межправительственных переговоров.

Заключения и рекомендации

15. В ходе дискуссии по проблеме киберпреступности был согласован ряд заключений и рекомендаций, а также выработано единое мнение о том, что государствам и международным организациям необходимо принять оперативные и конкретные меры по выполнению этих рекомендаций.

16. Участники дискуссии согласились с тем, что развитие технологий сопряжено как с преимуществами, так и с угрозами для общества, и что необходимо незамедлительно сосредоточить внимание на противодействии киберпреступности. В интересах разработки эффективных стратегий следует подробно проанализировать связи между технологиями и преступностью и способствующие их развитию факторы.

17. Государствам следует создавать и наращивать долгосрочный и устойчивый потенциал. Развивающиеся страны остро нуждаются в технической помощи, особенно в области наращивания потенциала и разработки законодательства, а также в материальных ресурсах и подготовке экспертов. ЮНОДК следует продолжить сотрудничество с ключевыми партнерами по линии оказания технической помощи в этом отношении, в том числе с Советом Европы, ответственным за решение вопросов, связанных с осуществлением Будапештской конвенции. Необходимо всесторонне рассмотреть вопрос о разработке плана действий по наращиванию потенциала на международном уровне.

18. Государствам следует приложить все усилия для развития сотрудничества между национальными учреждениями, между государствами и с частным сектором. Это требует полномасштабной политической приверженности со стороны правительств. Следует укреплять механизмы обмена информацией и наилучшими видами практики между государствами, в том числе путем развития соответствующих сетей.
