UNITED NATIONS INFORMATION SERVICE

Vienna International Centre
PO Box 500, 1400 Vienna, Austria
Tel: (+43-1) 26060-4666
Fax: (+43-1) 26060-5899
Email: unis@unvienna.org
http://www.unis.unvienna.org

Информационный бюллетень № 8

Дефицит международного сотрудничества позволяет киберпреступности оставаться безнаказанной

Быстро развивающийся и меняющийся характер информационных технологий, наряду со стремительно расширявшейся на протяжении последнего десятилетия «всемирной паутиной» и экспоненциальным ростом скорости обмена информацией, сделали расследование преступлений, совершаемых в киберпространстве, особенно нелегкой задачей. В конце 1997 г. лишь 1,7% мирового населения или 70 млн. человек пользовались Интернетом. Согласно последним данным Международного союза электросвязи (МСЭ), в 2009 г. число пользователей выросло до приблизительно 1,9 миллиарда, что составляет 26% населения мира.

Несмотря на растянувшееся на пять десятилетий обсуждение этой проблемы, использование информационно-коммуникационных технологий в преступных целях в последние годы по-прежнему является серьезным вызовом как для правоохранительных, так и законодательных органов. Международное сотрудничество в борьбе с электронной и киберпреступностью, принимая во внимание его значимость, поразительно слабо развито по сравнению с сотрудничеством в борьбе с «традиционной» преступностью.

Характер и масштабы проблемы

Глобальная доступность электронных и виртуальных услуг означает, что преступность в информационном пространстве естественным образом имеет транснациональное измерение. Даже в случает с отправкой простого электронного письма, отправитель и получатель которого находятся в одной и той же стране, присутствует транснациональный элемент, если один из них использует почтовую службу иностранного провайдера. Один лишь факт, что некоторые популярные почтовые сервисы имеют миллионы пользователей по всему миру, дает представление о масштабах, которые может принять киберпреступность.

Своевременное и эффективное сотрудничество между государствами имеет ключевое значение для обеспечения успешного расследования, ибо, в отличие от расследования традиционных уголовных дел, у следователей по делам о преступлениях в информационном пространстве в распоряжении имеется лишь очень короткий временной интервал. Огромные файлы могут быть скачаны за минуты! Определенные соглашения о взаимной правовой помощи уже заключены и действуют, однако необходимость в разработке процедур для быстрого реагирования и международного сотрудничества является исключительно острой.

Несмотря на почти всеобщее согласие по поводу того, что преступность в киберпространстве является насущной проблемой, требующий немедленного и согласованного реагирования, сами масштабы этой проблемы с трудом поддаются количественному измерению, не говоря уже о ее бесчисленных и постоянно видоизменяющихся реальных воплощениях. Даже основные национальные статистические сводки далеко не всегда фиксируют преступления в киберпространстве в виде отдельного вида преступлений. Таким образом, достоверную информацию о количестве задержаний, возбужденных судебных дел и вынесенных приговоров зачастую тяжело, а то и невозможно, получить.

О киберпреступности часто не сообщается по различным причинам. Например, пострадавшие – представители финансового сектора, такие как банки, могут не сообщать о предпринятых в их отношении хакерских атаках из-за страха утраты или ущерба своей репутации.

Важность создания глобальной сети оперативного реагирования

Тот факт, что преступления в информационном пространстве могут совершаться даже если преступники и объекты их атаки находятся в разных местах, делает чрезвычайно важным развитие государствами хорошо скоординированных механизмов сотрудничества. Вместе с тем, региональные расхождения в законодательстве о киберпреступности могут стать камнем преткновения: контент, признающийся противозаконным в одной стране, может быть легально размещен на сервере в другой стране. В

большинстве случаев взаимная правовая помощь оказывается на основе принципа обоюдного признания деяния преступлением, согласно которому преследуемое деяние должно быть уголовно наказуемым во всех затронутых странах. При наличии расхождений в законодательстве разных стран преследование киберпреступлений может быть существенно затруднено.

Лишить преступников безопасного убежища – ключевая задача предупреждения преступности в информационном пространстве. Безопасные убежища дают преступникам возможность осуществлять свою деятельность и чинить препятствия расследованиям. Один из примеров – компьютерный вирус «Love Bug», созданный на Филиппинах в 2000 г. и нанесший ущерб миллионам компьютеров по всему миру.

Связь организованной преступности и преступности в информационном пространстве
Вовлеченность организованной преступности в преступную деятельность в кибер-пространстве проявляется в двух формах: использование информационных технологий традиционными организованными преступными группами и «специализация» организованных преступных групп на совершении киберпреступлений.

Имеющиеся данные свидетельствуют, что основной является тенденции вовлечения традиционных организованных преступных групп в совершение преступлений в сфере высоких технологий, такие как незаконное распространение программного обеспечения, детская порнография и кража личных данных.

Предпринимаемые меры и нерешенные задачи
С целью развития и стандартизации законодательства в области борьбы с киберпреступностью был разработан ряд региональных инициатив, некоторые из которых описываются ниже.

Типовой закон стран Содружества о компьютерных и связанных с компьютерами преступлениях содержит положения уголовного и процессуального права и положения о международном сотрудничестве, распространяющиеся, однако, лишь на страны Содружества.

Евросоюз также разработал несколько подходов, включая Директиву об электронной торговле, Директиву о сохранении личных данных и Поправку к Рамочному решению о борьбе с терроризмом. Имплементация данных инструментов обязательна для всех 27 государств-членов ЕС.

Советом Европы разработаны три основных инструмента для гармонизации законодательства в сфере киберпреступности. Самый известный из них – Конвенция о киберпреступности, разработанная в период между 1997 и 2001 гг. Конвенция содержит положения из области материального уголовного права, процессуального права и положения о международном сотрудничестве. В 2003 г. был представлен первый дополнительный протокол к Конвенции о киберпреступности. В 2007 г. для подписания была открыты Конвенция Совета Европы о защите детей. Она содержит конкретные положения, признающие преступлением обмен детской порнографией, так же как и получение доступа к детской порнографии с использованием коммуникационных технологий.

Кроме того, существует несколько научных инициатив, таких как проект Стэнфордской Международной конвенции, разработанный по итогам конференции в Стэнфордском Университете (США) в 1999 г. и на основании Комплекта методических материалов МСЭ по законодательству в сфере киберпреступности, разработанного Американской ассоциацией адвокатов и другими экспертами. Несмотря на это, глобальное влияние таких инструментов ограничено, так как они применимы лишь в присоединившихся к ним государствах. На сегодняшний день Конвенция Совета Европы о киберпреступности имеет наиболее широкий охват: ее подписали 46, а ратифицировали 26 государств.

В связи с таким новым угрожающим общественной безопасности феноменом, как использование сети Интернет террористами в целях пропаганды, финансирования терроризма с помощью интернет-платежей и сбора информации о возможных целях террористической деятельности, необходимость совместных действий сейчас выше, чем когда-либо ранее.

Дополнительная информация:
www.unis.unvienna.org
www.unodc.org
www.crimecongress2010.com.br

Прямая веб-трансляция:
www.un.org/webcast/crime2010