

Многосторонний манифест

Приоритетность равноправия и справедливости в рамках предлагаемого Договора ООН по борьбе с киберпреступностью

Ландшафт современных киберугроз динамично меняется. Частота, изоцирненности и интенсивности кибератак растёт, угрожая нашей коллективной безопасности. Киберпреступность создает новые риски для безопасности, достоинства и равноправия людей. Самостоятельно противостоять таким угрозам на должном уровне невозможно. Для решения транснациональных проблем, связанных со злонамеренным использованием информационно-коммуникационных технологий (ИКТ), а также для защиты и обеспечения реализации прав пользователей, жизненно необходим подход основанный на привлечении всех заинтересованных сторон.

Мы внимательно следим за переговорным процессом по новой конвенции о киберпреступности в соответствии с [Резолюцией 74/247 Генеральной Ассамблеи Организации Объединенных Наций](#). Принимая во внимание существующие международные и региональные инструменты по борьбе с киберпреступностью, мы призываем международное сообщество избегать дублирования усилий и сосредоточиться на работе по обеспечению реализации и соблюдения установленных рамочных условий.

Тем не менее, признавая большинство голосов в Организации Объединенных Наций, мы излагаем ряд принципов, которым, по нашему мнению, должны следовать участники процесса в целях обеспечения прав и свобод, необходимых для создания свободного, открытого, безопасного и мирного киберпространства, а также обеспечения уважения к верховенству закона в киберпространстве.

Защита жертв

Основной целью нового международного закона о противодействии киберпреступности должна стать защита объектов и жертв киберпреступлений, а также предоставление эффективных средств правовой защиты и надлежащего комплекса гарантий в сфере прав человека. Правительства во всем мире уже давно злоупотребляют мерами по борьбе с киберпреступностью, используя законодательство о борьбе с киберпреступностью для расширения государственного контроля и криминализации публикации и распространения нежелательного контента, введения массовой слежки и ограничения частной жизни во имя борьбы с терроризмом. Новый договор должен обеспечить защиту безопасности, равноправия и достоинства людей в соответствии с обязательствами государства перед своими гражданами. В целях защиты жертв киберпреступлений любой будущий правовой документ должен гарантировать, что определения, квалифицирующие поведение как преступное, являются адаптируемыми и в то же время узкими для предотвращения криминализации поведения, представляющего собой осуществление основных свобод и прав человека.

Эффективная борьба с киберпреступностью путем обеспечения исполнения договоров международного сотрудничества

Главная цель новой конвенции ООН по борьбе с киберпреступностью должна заключаться в борьбе с киберпреступностью при одновременном утверждении приоритетности равноправия и справедливости. Краеугольным камнем нового договора должно стать эффективное применение существующих решений для обеспечения исполнения договоров международного сотрудничества между судебными и правоохранительными органами в условиях прозрачности надзора и соблюдения прав человека. В договоре следует признать, что расследование киберпреступлений и судебное преследование за их совершение требуют расширения межсекторального и международного сотрудничества, а также согласованности нормативных баз.

Соблюдение существующих международных правовых обязательств

Новый договор о борьбе с киберпреступностью не может быть использован государствами в качестве инструмента для сокращения их существующих обязательств по международному праву, особенно международному праву в области прав человека. В этом духе новый договор должен дополнять или упорядочивать, а не подменять существующие международно-правовые обязательства государств. Новый договор должен подтверждать существующие международно-правовые обязательства и основываться на разъяснении положительного влияния этих договорных обязательств.

Упор на механизмы подотчетности

Новая конвенция должна быть направлена на привлечение к ответственности на основе доказательств, что позволит лицам, пострадавшим от киберпреступлений, добиваться возмещения ущерба и использовать средства правовой защиты. Государствам необходимо сократить оперативное пространство для преступников не только применяя согласованные международные правовые нормы и взаимодействуя по вопросам судебного преследования, но и стимулируя государственно-частные партнерства бороться с киберпреступностью. При привлечении к ответственности виновных в причинении ущерба необходимо учитывать воздействие киберпреступности на общество в целом.

Долгосрочная актуальность договора

С учетом того что киберпреступность быстро развивается, определения должны соответствовать новым реалиям. Сфера применения новой конвенции должна быть четко определена и не зависеть от динамики развития технологий.

Сохранение открытости сети Интернет

Все большее число стран преследует цель разделить сеть Интернет на различные национальные сферы влияния и контроля. Новая конвенция по борьбе с киберпреступностью не должна служить оправданием или мотивом для того, чтобы недемократические режимы еще больше угрожали открытости сети Интернет,

закрывая свои цифровые границы для остального мира под предлогом предотвращения киберпреступности. Для обеспечения открытости сети Интернет новый договор должен предусматривать возможность корректировки юрисдикционных правил с учетом реалий глобализации сети Интернет и свободного потока информации.

ВНЕДРЕНИЕ НАДЛЕЖАЩИХ ПРОЦЕССОВ

Использование систематического многостороннего подхода

На всех этапах процесса должны проводиться конструктивные консультации с привлечением всех заинтересованных сторон. В рамках процесса необходимо учитывать интересы гражданского общества, экономики, ученых, исследователей, технических экспертов, научных и исследовательских учреждений. Для обеспечения необходимого баланса к переговорному процессу в числе других должны быть привлечены эксперты в области кибербезопасности, управления сетью Интернет, международного права и прав человека.

Содействие обеспечению прозрачности

Переговоры по предлагаемому договору должны быть максимально прозрачными. Организации, частные лица и государства, чьи интересы и права могут быть затронуты по результатам переговоров, должны иметь возможность представить свое мнение. Например, график и участники переговоров, а также тексты проектов документов должны быть доступны широкой общественности.

Уточнение сферы применения

Излишне широкое определение киберпреступности может привести к криминализации широкого круга видов деятельности, выходящих далеко за рамки собственно киберпреступлений. Участники переговоров должны четко определить рамки преступлений, для которых они стремятся предусмотреть меры наказания, чтобы гарантировать, что данный договор не может быть использован для оправдания репрессий против политической оппозиции, правозащитников или гражданского общества.

Принятие подхода, основанного на консенсусе

Новый договор о киберпреступности должен стать результатом подхода, основанного на консенсусе. Договор должен содержать положения, согласованные разнообразными странами и регионами и основанные на масштабных консультациях с соответствующими экспертами и группами заинтересованных сторон.

Самый новый перечень подписантов доступен на веб-сайте [CyberPeace Institute](http://CyberPeaceInstitute.org) или [Cybersecurity Tech Accord](http://CybersecurityTechAccord.org). Для получения дополнительной информации можно направить запрос на адрес электронной почты info@cyberpeaceinstitute.org или info@cybertechaccord.org