Альфредо Морелли, Представитель Аргентины в Группе Правительственных Экспертов ООН (ГПЭ ООН) по Достижению в сфере информатизации и телекоммуникаций в контексте международной безопасности, созданной согласно резолюции A/RES/53/70 (2012)

Процесс, который ведет ГПЭ ООН, хотя и держит на повестке дня очень важный вопрос, не окажет значительного влияния на решения по вопросам безопасности, принимаемые государствами. Можно было бы говорить о прогрессе, если бы страны открыто заявили о своем намерении начать обсуждать некоторую форму «цифрового сдерживания», чего мы не наблюдаем. Скорее наоборот, стремительно развиваются вооружения, в которых ИКТ являются ключевым элементом.

Об итогах работы четвертой Группы Правительственных Экспертов ООН (ГПЭ ООН) по Достижению в сфере информатизации и телекоммуникаций в контексте международной безопасности (2015) «Пульсу кибермира» рассказал Альфредо **Морелли,** Представитель Аргентины в третьей Группе Правительственных Экспертов ООН (ГПЭ ООН) по Достижению в сфере информатизации и телекоммуникаций в контексте международной безопасности, которая вела свою работу в 2012-2013 гг. Г-н Морелли поделился своими впечатлениями о резолюции ГПЭ, опубликованной в августе 2015г.: в ней отражены договоренности государств-участников по некоторым конкретным нормам поведения в киберпространстве, которых ранее не удавалось достичь, в том числе и предыдущей ГПЭ.

Каково Ваше общее впечатление от итогов работы 4-й ГПЭ ООН в сравнении с предыдущей, в которой работали Вы? В чем, по-Вашему, были совершены особенно важные шаги вперед и жизнеспособные соглашения?

Результаты работы группы достаточно неопределенные, чтобы каждый мог трактовать их так, как хочет. Группа недостаточно продвинулась в своей работе, на самом деле, сами угрозы развиваются гораздо быстрее, чем достигаются соглашения по борьбе с ними. Учитывая скорость роста количества рисков, угроз и инцидентов, необходимо ускорять и работу, которая должна в итоге привести нас к более безопасному, стабильному, глобальному и свободному киберпространству.

Основные концептуальные различия между подходами участников к информационной и кибербезопасности давно обозначены. Считаете ли Вы, что разногласия удалось несколько смягчить?

Полагаю, что был достигнут некоторый прогресс в различии «безопасности сетей» и «безопасности использования сетей». Во-вторых, это широкое признание применения международного права к киберпространству, пусть и пока концептуальное. В-третьих, признание важности мер укрепления доверия (CBMs), поддержания устойчивости сети и информационных потоков, обоснования обвинений в адрес стран, с чьих территорий были осуществлены кибератаки, важности неиспользования информации для вмешательства во внутренние дела других государств как части ответственного поведения стран. Все же, в целом, создается впечатление, что по разным вопросам кибербезопасности преимущество позиций США укрепилось.

Насколько эффективным, на Ваш взгляд, может быть техническое сотрудничество стран с учетом нынешней атмосферы недоверия на фоне геополитических проблем? Можно ли ожидать, что государства различных стран в самом деле будут делиться информацией об уязвимостях своей критической инфраструктуры?

Техническое сотрудничество никогда не достигнет уровня, которое могло бы представлять угрозу в ходе раскрытия информации, связанной с государственной безопасностью. Как и частный сектор, например, банковская отрасль, неохотно раскрывает информацию о совершенных на него кибератаках, государства не будут добровольно сообщать об уязвимостях объектов своей критической информационной инфраструктуры. Сотрудничество стран должно быть обращено к продвижению механизмов поддержки развивающихся стран (capacity building), ведь и документ [резолюция ГПЭ ООН — ред.] утверждает необходимость глобального подхода к вопросам безопасности. Страна, находящаяся на низком уровне обеспечения кибербезопасности, представляет собой угрозу для всех.

Ранее утверждалось, что группа могла бы быстрее договориться о ненападении на конкретные типы объектов критической инфраструктуры, такие как банковская или ядерная отрасль. Как Вы думаете, почему этого не произошло?

Дело в том, что каждая страна определяет для себя типологию объектов критической инфраструктуры в соответствии со своей экономической, политической и социальной системой. Поэтому более разумным видится общая формула, согласно которой «государства должны воздерживаться от атак на критическую инфраструктуру других государств».

По Вашему мнению, насколько принципиален спор вокруг особого упоминания 51-й статьи Устава ООН (гарантирующей государству право на самооборону в случае, если на него осуществлено вооруженное нападение), признание применимости которой Россия не хотела выносить в отдельное положение резолюции помимо общего признания применимости Устава ООН к киберпространству?

Легитимное право на самооборону в соответствии с 51-й статьей Устава ООН осложняется невозможностью точной атрибуции атак. Нельзя осуществить «законную самооборону», если нет уверенности в отношении источника атаки. Также нет и определения, что составляет атаку, которая приводит в действие положения статьи 51 (а не другие нормы международного права). То есть, при утверждении ее применимости к киберпространству остается неясным, как

именно она применяется. А утверждение, что страны могут принимать «меры», лишь увеличивает неопределенность.

Вы считаете, данные нормы будут в самом деле работать как средство сдерживания? Есть ли у них шанс приобрести со временем юридически обязующую силу, и что для этого необходимо?

Строго говоря, добровольные нормы являются не нормами, а *рекомендациями* [курсив — ред.]. Политические соглашения сегодня в моде, поскольку страны не могут взять на себя никаких обязательств. В моем представлении это демонстрация популизма и нехватка лидерства в некоторых странах. В любом случае эти соглашения позволят пристыдить те государства, которые не будут следовать договоренностям. При этом есть риск предвзятости при оценке действий тех или иных стран. Тот процесс, который ведет ГПЭ ООН, хотя и держит на повестке дня очень важный вопрос, не окажет значительного влияния на решения по вопросам безопасности, принимаемые государствами. Можно было бы говорить о прогрессе, если бы страны открыто заявили о своем намерении начать обсуждать некоторую форму «цифрового сдерживания», чего мы не наблюдаем. Скорее наоборот, стремительно развиваются вооружения, в которых ИКТ являются ключевым элементом.

Насколько реалистичны договоренности о нераспространении «злонамеренных программных и технических средств в сфере ИКТ и использования пагубных скрытых функций» с учетом уже давно известных практик «государственно-частного партнерства» в различных странах по внедрению закладок в продукты ИКТ?

Важно глубже изучать роль и ответственность частного сектора в отношении всех форм деятельности в области ИКТ. Поскольку государства используют частные компании как инструменты своей политики безопасности, предложение воздержаться от использования «скрытых функций» в продуктах ИКТ пока видится декларативным обозначением желаемого.

Есть ли стороны, непосредственные «выигравшие» от данного соглашения?

Данная дискуссия происходит прежде всего между ведущими державами. Для развивающихся стран политическая нестабильность очень нежелательна. У них мало ресурсов, а те, что имеются, желательно использовать для развития, а не для военных целей. В любом случае, полагаю, что проблема не в государствах, которые, в конце концов, согласуют «modus vivendi», а в негосударственных акторах, которых сложно контролировать, ведь тот рынок, в котором они оперируют, гораздо прибыльнее. Если не появятся механизмы их сдерживания, проиграем мы все.

Вопросы и перевод с испанского - А. Куликова