

**A Global Treaty on Cybersecurity and Cybercrime. Second edition. 2011, Stein Schjolberg and Solange Ghernaoui-Helie. ISBN 978-82-997274-3-3 (elektronisk). Printed by AiTOslo 2011.**

Плод совместного авторства норвежца Штайна Шольберга и его швейцарской коллеги, г-жи Соланж Гернутти-Эли под названием «*Всеобщий договор о кибербезопасности и киберпреступности*» трудно причислить к какому-либо определенному жанру. Формально речь идет о втором издании рабочего проекта всеобъемлющего международно-правового акта ООН, посвященного вопросам международной координации борьбы с киберпреступностью и обеспечения безопасности в киберпространстве. Проект договора, насколько можно судить, подготовлен по самостоятельной инициативе авторов; рассматривать его следует отдельно от инициатив самой ООН в данной сфере, хотя его авторы принимали непосредственное участие в развитии этих инициатив.

Однако определение *рабочий проект* несколько искажает и принижает суть труда – скорее, речь идет о доктринальной разработке, претендующей на глобальные нововведения в международно-правовой области, связанной с киберпространством. Сухой и лаконичный формат самого *проекта Договора* (всего 23 статьи) органично дополняет часть за авторством Гернутти-Эли, где излагается общее видение и принципы, на которые опирается каждая из статей будущего международного-правового акта. В итоге суммарное смысловое наполнение документа способно дать фору многим научным монографиям – к слову сказать, в библиографиях обоих авторов данная публикация отнесена к этому типу работ, а не к докладам.

Между тем, рассказывая о самом проекте, необходимо еще раз вернуться к его авторам – прежде всего как к лицам, обладающим исключительной компетенцией и опытом в той проблематике, которую затрагивает *Договор*. Профессор Штайн Шольберг в 2007-2008 гг. занимал пост Председателя Группы Экспертов Высокого Уровня по Кибербезопасности (High Level Expert Group on Cybersecurity), учрежденной в 2007 г. как раз для изучения возможностей выработки всеобщего документа по киберпреступности в рамках ООН.<sup>1</sup> Деятельность Группы должна была дополнять Глобальную повестку в области киберпреступности (Global Cybercrime Agenda) при Международном союзе электросвязи (МСЭ), старт которой был дан в том же 2007 г.

Таким образом, профессор Шольберг не только является крупнейшим и одним из старейших норвежских экспертов в области киберправа, но и одной из центральных фигур, задействованных в продвижении инициатив ООН по международно-правовому регулированию сферы кибербезопасности. В свою очередь, Соланж Гернутти-Эли, профессор Университета Лозанны, претендует на звание крупнейшего в своей стране теоретика киберправа. На этом фоне тем удивительнее тот факт, что оба автора вообще незнакомы русскоязычному

---

<sup>1</sup> The High-Level Experts Group on Cybersecurity (HLEG). ITU Official Website. <http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html>

читателю – всемогущему Google неизвестны даже их имена на русском языке, не говоря уже о переводах трудов.

Между тем – и вряд ли случайно, - появление документа (как первого, так и второго изданий) приходится на то время, когда активно разгорается дискуссия по поводу перспектив международно-правового регулирования преступности в киберпространстве, да и кибербезопасности в целом. И центральное место в этой дискуссии занимает РФ, которая пытается представить альтернативу Будапештской конвенции 2001 г., отдельные статьи которой оказались для нее неприемлемы.<sup>2</sup> Пока баталию за право продвигать на глобальном уровне собственное видение всеобщего документа по киберпреступности Россия скорее проигрывает – за 2009-2011 гг. инициатива Москвы не нашла поддержки в БРИКС, а ЕС и США в основном предпочитают отстаивать преимущества Будапештской конвенции. В то же время, ограниченность регулирующего потенциала последней становится несколько более очевидной с течением времени. В этом смысле запуск инициатив МСЭ, включая Глобальную программу кибербезопасности (ГПК) свидетельствует о том, что и страны Запада в рамках ООН ведут разработку универсальной альтернативы Конвенции Совета Европы, и вопрос состоит скорее в том, чьим интересам новый документ будет соответствовать в большей степени.

Одной из центральных идей в *проекте* является утверждение всеобъемлющего, комплексного подхода к регулированию киберпреступности в международном праве. Авторы (в первую очередь профессор Гернутти-Эли) провозглашают неотъемлемый характер, принципиальную важность формирования *культуры кибербезопасности*, адаптации общей стратегии борьбы с киберпреступностью к локальному контексту, взаимосвязи кибербезопасности с общим потенциалом развития той или иной территории, региона. Такой подход по-новому открывает смысл *всеобщего* Договора – речь идет не только о глобальном масштабе действия и применения новых норм, но и выработке мер системного, междисциплинарного регулирования тех сфер жизни общества, которые Кибербезопасность, на первый взгляд, может не касаться напрямую.

Яркой новацией в проекте является стремление его авторов *модернизировать* существующее наднациональное законодательство в сфере кибербезопасности – и в том числе Конвенцию Совета Европы 2001 г. «О киберпреступности», уже на уровне официальной терминологии. Авторы заостряют внимание на том, что за прошедшие с разработки конвенции годы перечень и структура киберпреступлений существенно изменились – обострились угрозы, связанные с распространением порнографии, присвоением виртуальной идентичности, кибертерроризмом и масштабными кибератаками. В связи с этим базовый

---

<sup>2</sup> Речь идет, прежде всего о пресловутом пункте Б статьи 32 Конвенции Совета Европы «О киберпреступности» от 2001 г. В соответствии с положениями пункта компетентные органы стран-участниц Конвенции могут при определенных условиях получать доступ к данным в российских сетях, не согласовывая его с российскими структурами. Резкое неприятие этот пункт вызвал прежде всего у российских спецслужб, включая ФСБ. По сей день перспектива присоединения РФ к Будапештской конвенции остается предметом открытой дискуссии в российских властных кругах.

гlossарий Конвенции нуждается в обновлении, которое и предлагают Шольберг и Гернутти-Эли, вводя собственные определения киберпреступлений.

Вместе с тем, создается впечатление, что *новые вызовы кибербезопасности*, которым авторы уделяют особое внимание в предисловии проекта, не получают ожидаемого внимания и проработки в самих его статьях. Так, угрозе терроризма в киберпространстве и масштабным кибератакам посвящено по одной статье, причем в одной из оба явления *свалены в кучу* и рассматриваются вместе.

Здесь стоит упомянуть о, наверное, наиболее очевидном недостатке всего проекта (не менее характерного для прилагающейся концепции): тщась *объять необъятное* и втиснуть в один договор регулирование всех аспектов киберпреступности и кибербезопасности вообще, авторы зачастую упускают из виду конкретику. Во многом неопределенность положений проекта и аморфный характер границ предмета его регулирования заложены уже в его названии. Строительство международно-правового регулирования киберпространства на базе документа, нацеленного одновременно на киберпреступность и, в то же время, на всю сферу кибербезопасности – задача странная и не вполне логичная. Так что, возможно, золотые дни Будапештской конвенции еще впереди, а у РФ будет шанс продать свой вариант всеобщего договора о киберпреступности (*или кибербезопасности*).

Но вместе с тем, невзирая на противоречия и недостатки, объективно присущие любому рабочему проекту подобного уровня, работа профессора Шольберга и профессора Гернутти-Эли обязательна к изучению всем тем, кто интересуется международной повесткой кибербезопасности – и тем более тем, кто изучает эту проблематику с точки зрения интересов России.