мог выступать с законодательной инициативой, осуществлял руководство нижестоящими прокурорами, контролировал фискальную службу, отслеживал исполнение высочайших предписаний.

В соответствии с указами прокуратура получила особый статус надзорного органа. Прокурор мог реагировать на незаконные акты и поступки в форме опротестования. Опротестование представляло собой устное разъяснение законодательства и предложение устранить допущенное нарушение закона, в случае если это не приносило результата, то предусматривалось письменное опротестование. В ситуации продолжавшегося неисполнения законных требований прокурор имел право обратиться с донесением непосредственно к генерал-прокурору, а генерал-прокурор в свою очередь мог обратиться напрямую к монарху.

11 мая 1722 г. император распорядился образовать прокуратуру также при Святейшем Правительствующем Синоде. При этом прокуратура разделялась, в свою очередь, на два уровня: первый уровень составляли высшие надзорные учреждения – Генерал-прокуратура Сената и Обер-прокуратура Синода, второй – нижестоящие прокуратуры центральных ведомств и надворных судов.

Следует также отметить особый статус прокуратуры, который заключался в ее независимости и подчиненности генерал-прокурора и обер-прокурора непосредственно императору. В законодательстве было закреплено, что судить генерал-прокурора и обер-прокурора имел право только монарх, при этом Сенату была дана возможность пресечения противоправных деяний, совершаемых прокурорами.

Таким образом, следует отметить, что роль прокуратуры в государственном аппарате Российской империи при Петре I была столь велика, что генерал-прокурор в некотором смысле становился выше Сената. Несмотря на то что прокурор не имел права решающего голоса ни по одному административному вопросу, авторитет прокуратуры поддерживался особым отношением к ней Петра I, который наделил прокуратуру особым статусом и правом от его имени и по его поручению осуществлять надзор и контроль за деятельностью Сената и других государственных органов.

УДК 341.32

Р.А. Середа

МЕЖДУНАРОДНОЕ ГУМАНИТАРНОЕ ПРАВО В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: КИБЕРВОЙНА КАК НОВАЯ СРЕДА ПРИМЕНЕНИЯ

Развитие цифровых технологий в последние десятилетия оказывает беспрецедентное влияние на все сферы жизнедеятельности общества и государства. Виртуальное пространство сети Интернет становится альтернативной средой для функционирования многих государственных институтов, включая такие жизненно важные системы, как энергетика, транспорт, торговля, связь и коммуникации, банковская система. Как следствие, от эффективности работы данных институтов в киберпространстве все больше попадает в зависимость как национальная безопасность, так и возможность реализации основополагающих прав и свобод человека.

Закономерным является и то обстоятельство, что по мере нарастания значимости киберпространства для реализации государственных функций оно все чаще становится новой средой для противоправных посягательств на государственный суверенитет со стороны злоумышленников и противников действующей власти. И если в мирное время подобные действия подпадают в сферу общеуголовной преступности и борьба с ними регламентируется национальным законодательством, то в условиях международных вооруженных конфликтов возникает ряд вопросов относимости кибератак военного характера и их последствий к сфере регулирования международного гуманитарного права (МГП).

МГП, также известное как «право войны», накладывает на страны, ведущие военные действия, определенные ограничения, направленные на защиту гражданского населения, медицинского персонала, раненых и военнопленных. В соответствии со ст. 51 Дополнительного протокола к Женевским конвенциям от 12 августа 1949 г., касающегося защиты жертв международных вооруженных конфликтов (далее – ДП), запрещается нападение на гражданское население. Ст. 51 и 54 ДП отдельно предусматривают защиту от нападений на гражданские объекты и объекты, необходимые для выживания гражданского населения. Ввиду этого важнейшим вопросом, требующим обсуждения, является применимость вышеуказанного термина «нападение» к кибератакам в цифровой среде.

В соответствии со ст. 49 ДП под нападением понимаются акты насилия в отношении противника независимо от того, совершаются они при наступлении или обороне, применительно к любым военным действиям на суше, в воздухе или на море. Очевидно, что буквальное толкование данной нормы может необоснованно исключать кибератаки из категории «нападение», так как они проводятся в виртуальном пространстве, несмотря на то что ими может быть причинен значительный ущерб гражданскому населению.

Следует согласиться с мнением Международного Комитета Красного Креста, который причисляет к нападениям те кибероперации, которые могут привести к гибели, ранениям или физическому ущербу среди гражданского населения. Причем сюда необходимо относить как прямые последствия кибератаки (крушение самолета в результате взлома системы управления полетами), так и ее косвенные последствия (гибель пациентов больницы по причине отключения электропитания после кибератаки на электростанцию). При этом полагаем, что все военные кибероперации, которые направлены на нарушение работы гражданской инфраструктуры (банковская система, система связи и услуг), даже при отсутствии физического ущерба, должны быть причислены к нападению с признанием соответствующих ограничений, предусмотренных МГП.

В свою очередь, проблемным вопросом является реализация принципа избирательности при проведении военных кибероперациий. Согласно ст. 51 ДП запрещено использование видов вооружений неизбирательного типа, воздействие которых не может быть ограничено только военными целями. Следует признать, что в своем большинстве кибератаки имеют избирательный характер, поскольку планируются и осуществляются применительно к конкретным объектам информационной инфраструктуры. Вместе с тем в условиях цифровой глобализации весьма сложно спрогнозировать весь каскад возможных последствий, которые могут затронуть неопределенный круг лиц. Например, спутниковая система связи, используемая вооруженными силами, является законным объектом нападения. Однако выведение из строя спутника может повлечь сбои в работе гражданских экстренных служб, что причинит неизбирательный ущерб гражданскому населению.

Кроме того, неизбирательным действием могут обладать такие средства ведения разведки и кибероперациий, как распространение вредоносных программ, которые изначально спроектированы для самостоятельного и неизбирательного воздействия на широкий круг компьютерных систем. В результате в условиях сети Интернет атака с применением данных средств на конкретную систему может привести к неизбирательным последствиям. Таким образом, полагаем, что при создании соответствующих инструментов проведения кибератак в условиях вооруженных конфликтов необходимо учитывать соответствующие нормы МГП.

Отдельного внимания заслуживает вопрос о применимости тех либо иных статусов, предусмотренных МГП (комбатант, военнопленный, наемник и др.), к лицам, причастным к осуществлению кибератак и операций в условиях вооруженного конфликта международного характера. Речь идет о тех случаях, когда указанные действия совершаются лицами, не входящими в состав вооруженных сил, а во многих случаях находящимися за пределами воюющих государств и не являющимися их гражданами.

Например, 26 февраля 2022 г. правительство Украины призвало хакеров-любителей всего мира присоединиться к его «ИТ-армии» и начать атаки против российских целей. Всемирно известный хакерский коллектив Anonymous в первый же день войны объявил, что тоже начнет кибервойну против России.

Полагаем, что в случае расширительного толкования ст. 13 Женевской конвенции от 12 августа 1949 г. «Об улучшении участи раненых и больных в действующих армиях» участники такой «ИТ-армии», которые являются гражданами Украины либо находящиеся на ее территории, могут быть причислены к комбатантам. Однако при этом на них должны распространяться обязанности по соблюдению норм МГП.

Сходного мнения придерживается заместитель директора женевской неправительственной организации Cyber Peace Institute Бруно Халопо. По его мнению, эти кибервоины не осознают, что их участие в конфликте регулируется МГП. Принимая активное участие в этом конфликте, они могут утратить правовой статус гражданского лица и оказаться в положении комбатантов. Тем самым они рискуют подвергнуться ответному удару со стороны государства, на объекты которого они нападают, и стать после войны субъектами потенциального судебного разбирательства. В свою очередь, действия лиц, принимающих участие в подобных кибероперациях из корыстной заинтересованности, должны подпадать под признаки наемничества, а сами лица – привлекаться к юридической ответственности.

Таким образом, в условиях развития новых способов достижения военных целей в условиях международных вооруженных конфликтов требуют переосмысления и совершенствования подходы МГП к ограничению средств проведения кибероперациий, целей, на которые они могут быть направлены, а также определения статуса лиц, принимающих участие в проведении кибератак военного характера.

УДК 340.114.5

Е.И. Стабровский

ЗНАЧЕНИЕ ПРАВОВОГО СОЗНАНИЯ ПРАВОПРИМЕНИТЕЛЯ: АНТРОПОЛОГО-ПРАВОВОЙ АСПЕКТ

Перспективным направлением совершенствования деятельности по формированию правосознания правонарушителей является обращение к правовому сознанию правоприменителя. Ввиду универсальности структуры правового сознания личности его содержательные характеристики у правоприменителя должны быть максимально устойчивыми на бытийном уровне (правовые эмоции, чувства и пр.), максимально развитыми на рефлексивном уровне (правовые знания, представления, нормативные правовые ценности и пр.) и максимально принятыми на личностно-ценностном уровне (личностные правовые ценности).

Правоприменителю в процессе реализации юридической ответственности в отношении правонарушителя необходимо стремиться к достижению установленных законодательством целей. В случае отсутствия соответствующих характеристик правового сознания правоприменителя и необходимости их формирования у правонарушителя успешная реализация юридической ответственности в виде исправления становится затруднительной.

Отсутствие требуемых характеристик правового сознания у конкретного правоприменителя может быть компенсировано за счет привлечения к формирующей деятельности другого правоприменителя. Также возможные сложности в деятельности правоприменителя, связанные с его правовым сознанием, могут быть компенсированы путем дополнительного законодательного регулирования, не требующего осуществления усмотрения, в том числе локальными актами, а также с помощью участия вышестоящих должностных лиц и соответствующих органов. Вышестоящие государственные органы конкретизируют пределы усмотрения и таким образом обеспечивают соблюдение установленных законодательством требований.

Вместе с тем значение правового сознания правоприменителя при реализации юридической ответственности не уменьшается. Реализация юридической ответственности во многом связана с вынесением решений, требующих усмотрения. Особенно