

# Изменение роли многосторонних форумов в урегулировании вооруженных конфликтов в цифровую эпоху

## **Амандип С. Гилл**

Амандип С. Гилл — директор международной совместной инициативы проведения исследований в области цифрового здоровья и ИИ при Программе по глобальному здравоохранению Женевского института международных исследований и развития. До августа 2019 года занимал пост исполнительного директора и одного из руководителей секретариата Группы высокого уровня по цифровому сотрудничеству при Генеральном секретаре Организации Объединенных Наций. Выступал в качестве посла и постоянного представителя Индии на Конференции по разоружению в Женеве. С 2017 по 2018 год был председателем Группы правительственных экспертов по новым технологиям в сфере смертоносных автономных систем вооружений в рамках Конвенции о запрещении или ограничении применения конкретных видов обычного оружия. На данный момент входит в состав специальной группы экспертов ЮНЕСКО по составлению рекомендаций об этике искусственного интеллекта и комиссии журнала «Ланцет» и газеты «Файнэншл таймс» «Управление будущим здравоохранения до 2030 года: взросление в цифровом мире».

## Аннотация

*В настоящей статье исследуется выборка многосторонних форумов, которые занимаются проблемами безопасности, возникающими в связи с цифровыми технологиями, в том числе кибервойнами, киберпреступностью и смертоносными автономными системами вооружений (САС)<sup>1</sup>. В статье определены структурные вопросы, которые затрудняют многосторонним форумам обсуждение быстро меняющихся цифровых проблем и своевременное реагирование на них посредством выработки необходимых норм и политических мер. Опираясь на анализ этой проблемы и недавний опыт регулирования киберконфликтов и САС в составе Группы правительственных экспертов, автор статьи предлагает схему многостороннего управления цифровыми технологиями в условиях вооруженного конфликта. В схеме содержится эвристический алгоритм для понимания взаимодействия «человек — машина», что позволит привлечь виновных к ответственности в рамках принципов международного гуманитарного права и международного права вооруженных конфликтов в цифровую эпоху. В заключение автор приводит конкретные предложения по содействию работе многосторонних форумов, занятых проблемами кибероружия и автономности смертоносных систем вооружений.*

**Ключевые слова:** цифровые технологии, конфликт, информационная безопасность, автономное оружие, интерфейс «человек — машина», распределенное управление, многосторонние форумы, международное гуманитарное право, привлечение к ответственности.



## Введение

Стабильность и безопасность в мире все сильнее переплетаются с цифровыми технологиями, и даже киберпотенциал старого поколения «становится более прицельным, воздействует на физические системы и исподволь подрывает общественное доверие»<sup>2</sup>. Проблема вышла за пределы физического поражения критически важных объектов инфраструктуры — портов, авиадиспетчерских служб, линий электропередачи и инструментов движения денежных средств — в результате кибератак и разрослась до «взлома» института общественного мнения и политических учреждений. Меры по выработке международных норм ответственного поведения, наращиванию потенциала и укреплению доверия остаются разрозненными, особенно

- 1 В понимании автора цифровые технологии представляют собой устройства, платформы, хранилища данных и архитектуру их обработки, алгоритмы, языки программирования, протоколы и стандарты связи, которые опираются на представление информации в виде дискретных двоичных значений. Информационно-коммуникационные технологии (ИКТ) — еще один термин, который может использоваться как синоним предыдущего.
- 2 High-Level Panel on Digital Cooperation, *The Age of Digital Interdependence: Report of the UN Secretary-General's High-Level Panel on Digital Cooperation*, June 2019, p. 27.

на межгосударственном уровне. Нормы, за которые выступает та или иная сторона, часто узконаправленны и не набирают критической массы поддержки от ключевых государств. Во многих юрисдикциях, таких как США и Европейский союз, отсутствие сотрудничества на международном уровне вызывает раздражение, и в ответ на кибератаки они все чаще в одностороннем порядке вводят санкции в отношении конкретных лиц и учреждений<sup>3</sup>. Это недоверие усугубляется введением адресных мер экспортного контроля, антимонопольной и инвестиционной политики, направленных на цифровые компании других сторон<sup>4</sup>.

С появлением искусственного интеллекта (ИИ) регулирование вооруженных конфликтов в цифровую эпоху дополнилось еще одним важным направлением. В результате соединения трех тенденций, а именно — увеличения вычислительной мощности, получения наборов больших данных через интернет и снижения стоимости хранения и обработки данных — такие инструменты ИИ, как машинное обучение, обрели большую популярность. Системы ИИ способны справляться с задачами, которые раньше решались исключительно людьми. Ярким примером является поражение восемнадцатикратного чемпиона мира по настольной игре го Ли Седоля, которое он потерпел в марте 2016 года в состязании с алгоритмом ИИ, разработанным DeepMind<sup>5</sup>. В частности, применение систем ИИ, основанных на машинном обучении, в вооруженных конфликтах вызывает опасения по поводу утраты контроля и надзора за ведением боевых действий со стороны человека<sup>6</sup>. Это может привести к причинению вреда гражданскому населению и комбатантам в условиях вооруженных конфликтов в нарушение международного гуманитарного права (МГП), а также вызвать новый виток гонки вооружений и снизить порог применения силы.

Пригодны ли многосторонние форумы для регулирования вооруженных конфликтов в цифровую эпоху? Для ответа на этот вопрос в настоящей статье сначала приводится исторический контекст современных многосторонних форумов, которые занимаются предотвращением конфликтов и контролем вооружений. Затем сложившиеся процедуры и результаты деятельности таких форумов сопоставляются с природой цифровых технологий и уникальными характеристиками их применения в условиях вооруженных конфликтов. Далее приводится обзор отдельных форумов, которые занимаются устранением последствий применения таких технологий. В частно-

3 Patryk Pawlak and Thomas Biersteker (eds), *Guardian of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace*, Chaillot Paper 155, EU Institute for Security Studies, October 2019.

4 Ana Swanson, “U.S. Delivers Another Blow to Huawei with New Tech Restrictions”, *New York Times*, 15 May 2020; Li Sikun, “China Ready to Target Apple, Qualcomm, Cisco and Boeing in Retaliation against US’ Huawei Ban: Source”, *Global Times*, 15 May 2020.

5 Amandeep S. Gill, “The Role of the United Nations in Addressing Emerging Technologies in the Area of Lethal Autonomous Weapons Systems”, *UN Chronicle*, Vol. 55, No. 3–4, 2019.

6 Генеральный секретарь ООН призвал запретить машины, способные выбирать цели и уничтожать людей без вмешательства человека. António Guterres, “Remarks at the ‘Web Summit’”, Lisbon, 5 November 2018, доступно по адресу: [www.un.org/sg/en/content/sg/speeches/2018-11-05/remarks-web-summit](http://www.un.org/sg/en/content/sg/speeches/2018-11-05/remarks-web-summit) (все ссылки на интернет-ресурсы приводятся по состоянию на январь 2021 г.).

сти, в статье рассматривается Группа правительственных экспертов (ГПЭ) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, с 1998 года периодически созываемая Генеральной Ассамблеей Организации Объединенных Наций (ГПЭ ООН), и ГПЭ, состоящая из всех высоких договаривающихся сторон Конвенции о запрещении или ограничении применения конкретных видов обычного оружия и с 2016 года занимающаяся вопросами смертоносных автономных систем вооружений (САС). Механизм определения подотчетности человека в рамках национального и международного права на разных этапах разработки и применения автономных цифровых технологий из этого обзора исключен. В завершение статьи намечаются некоторые направления будущей деятельности многосторонних форумов, которые занимаются проблемами конфликтов в сфере информационной безопасности и автономных вооружений, и предлагаются конкретные меры многостороннего управления цифровыми технологиями в контексте международной безопасности за счет кооптирования дополнительных субъектов управления и использования многоступенчатого подхода к применению норм.

## Исторический фон и контекст

С исторической точки зрения идея предотвращения и регулирования конфликтов еще до их возникновения, в мирное время, силами международных конференций и форумов является относительно новой. Можно считать, что она возникла в ходе послевоенных конференций 1863–1864 годов и 1868 года в Женеве, где были кодифицированы правила ведения боевых действий на суше и на море<sup>7</sup>, составления Санкт-Петербургской декларации, запрещающей применение в конфликтах определенной категории боеприпасов<sup>8</sup>, а также ряда мирных конференций, проведенных в Гааге в 1899 и в 1907 годах. Конференции в 1899-м и 1907-м стали «первыми подлинно международными собраниями, проходившими в мирное время в целях сохранения мира»<sup>9</sup>. Их наследие остается с нами и по сей день, например в форме Постоянной палаты третейского суда, которая обеспечивает площадку для арбитражных разбирательств, расследований и примирения государств в связи с соглашениями, в которые они вступили, и знаменитой оговорки Мартенса, выступающей ориентиром за пределами правовых норм гуманитарной защиты в ходе вооруженных конфликтов<sup>10</sup>.

7 По итогам первой из них был учрежден Международный Комитет Красного Креста (МККК) и принята Конвенция об улучшении участи раненых в действующих армиях от 22 августа 1864 г. Благодаря последней принципы Женевской конвенции 1864 г. были распространены на ведение боевых действий на море.

8 Санкт-Петербургская декларация о запрещении употребления разрывных пуль, Санкт-Петербург, 29 ноября и 11 декабря 1868 г.

9 James Brown Scott, “Prefatory Note”, *The Proceedings of the Hague Peace Conferences: Translation of the Official Texts: The Conference of 1899*, Oxford University Press, Oxford, 1920, p. v.

10 Theodor Meron, “The Martens Clause, Principles of Humanity, and Dictates of Public Conscience”, *American Journal of International Law*, Vol. 94, No. 1, 2000.

Последующие форумы, такие как Генеральная Ассамблея ООН и Военно-штабной комитет, вспомогательный орган Совета Безопасности ООН, отражают относительно скромные положения Устава ООН по поводу предотвращения конфликтов, разоружения и контроля вооружений по сравнению, например, с Уставом Лиги Наций, который в большей степени опирался на совместные действия в сфере разоружения и установления мира на планете<sup>11</sup>. Устав ООН также можно назвать «доядерным», поскольку его положения согласовывались до широкого распространения знаний о ядерном оружии. Разработка ядерного оружия и гонка вооружений периода холодной войны еще больше отвлекли на себя внимание от контроля обычных вооружений, которые в ту эпоху чаще играли второстепенную роль по сравнению со стратегическими вооружениями и воспринимались в региональном, а не в мировом масштабе. Эта разница в отношении к оружию массового поражения и к обычным вооружениям сохранилась даже несмотря на то, что в конце 1990-х годов произошел сдвиг тенденций в сфере технологий и безопасности, в результате которого значение обычных вооружений выросло. Изменение неосязаемых характеристик систем вооружений, в частности цифровизация их ключевых составляющих, тоже практически не привлекло внимания за пределами узкого круга практикующих специалистов в сфере режимов экспортного контроля, таких как Вассенаарские договоренности. Отставание политики от стремительного развития технологий после холодной войны очевидно и из непоследовательного применения терминов «кибербезопасность», «сетевая безопасность», «информационная безопасность» и «цифровая безопасность» — разработчики политики не очень хорошо представляли себе, с чем имеют дело, и пользовались тем выражением, которое было больше на слуху.

## Вызов цифровых технологий многосторонним форумам

Важно отметить, что цифровой переворот был не таким резким, как ядерный. Практикующие специалисты в сфере урегулирования конфликтов и контроля вооружений не сразу поняли, что имеют дело с принципиально новой технологией. В 1970-х годах об интернет-протоколах имела представление буквально горстка посвященных, но уже в 1984-м все интернет-хосты перешли на единый протокол управления передачей данных/интернет-протокол (TCP/IP), а в 1989 году в Женевском ЦЕРНе была изобретена Всемирная паутина, что положило начало стремительному внедрению цифровых коммуникационных сетей во всем мире. На базе виртуальной инфраструктуры, созданной за счет этой распределенной и масштабируемой системы, стало разворачиваться огромное количество приложений. Союз интернета и телефонии в начале XXI века освободил пользователей

11 Leland M. Goodrich, Edward Hambro and Anne Patricia Simons, *Charter of the United Nations: Commentary and Documents*, 3rd revised ed., Columbia University Press, New York, 1969.

от привязки к специально оборудованным рабочим местам, а социальные сети позволили создавать контент в небывалом объеме. Разумеется, среди этого контента были и спам, и побуждение к ненависти и насилию, и вредоносные программы. Цифровые сети обеспечили беспрецедентный уровень анонимности при создании и потреблении контента, глобальный охват сети Интернет позволил стремительно распространять этот контент, а огромная значимость доступа к интернету и его использования породила стимулы к масштабным злоупотреблениям.

Почему это имеет такое значение в контексте МГП и контроля вооружений? Сила традиционно ассоциируется с физическим уничтожением, причинением увечий и смерти, и мало кто мог себе представить, что нематериальное уничтожение или материальные последствия нематериальных нападений могут быть настолько серьезными, что будут квалифицироваться как вопросы международной безопасности. В дальнейшем, если и возникала необходимость регулировать распространение вводящей в заблуждение информации и пропаганды, речь шла об узком контексте использования военных хитростей или некорректного применения символов нейтралитета и защиты. Никому не приходило в голову, что дезинформация и искажение посылов и деятельности [национальных и международных] институтов с помощью цифровых технологий могут достичь таких масштабов. Остальные твердо определенные разграничения — между комбатантами и некомбатантами, между гражданскими и военными целями — тоже были поколеблены или даже нарушены. Наконец, хотя отклонения от стандартов допускались на протяжении всей истории МГП и контроля вооружений, практикующие специалисты всегда исходили из того, что определить источник применения силы несложно. Но как установить виновного, когда на спусковой крючок нажимало столько людей, причем многие неосознанно, и даже нет уверенности в том, был ли вообще этот спусковой крючок?

Рассмотрев трудности концептуального характера, обратимся к практическим проблемам. Традиционно многосторонние форумы обеспечивают урегулирование конфликтов за счет содействия обсуждению норм, регламентирующих, ограничивающих или исключаящих применение в ходе боевых действий конкретных сил и средств, а также за счет побуждения к диалогу и установлению доверия между потенциальными противниками. Одна из категорий таких форумов — хотя и малочисленная — позволяет государствам прояснять неоднозначные ситуации, выявлять нарушения и урегулировать разногласия до перехода в стадию конфликта<sup>12</sup>. Инструментарий таких форумов, применяющийся ими при выработке норм, заключается в комплексе мер, позволяющих осуществлять обмен информацией, обеспечивать прозрачность, делать заявления о нали-

12 В качестве примера можно привести расследование, проведенное Международным агентством по атомной энергии (МАГАТЭ) в отношении иранской программы обогащения урана посредством центрифугирования. IAEA, "Verification and Monitoring in Iran", доступно по адресу: [www.iaea.org/newscenter/focus/iran](http://www.iaea.org/newscenter/focus/iran).

чии объектов и запасов, проверять отсутствие определенных видов деятельности и предметов, а также соблюдать договоренности и вводить санкции за их нарушение<sup>13</sup>. В столь высокотехнологичных сферах, как космонавтика, химия, биология и ядерная физика, которые могут использоваться как в военных, так и в гражданских целях, многосторонние договоренности, например Режим контроля за ракетными технологиями, регламентируют передачу технологий с помощью требования придерживаться перечней контролируемых технических средств и выполнять руководящие принципы, ограничивающие экспорт в целях предотвращения использования технологий гражданского назначения для военных нужд<sup>14</sup>.

Однако цифровые технологии создают уникальные проблемы для практикующих специалистов в составе таких форумов<sup>15</sup>. Вопрос о том, что именно представляет собой инструмент конфликта, не имеет очевидного ответа, а традиционный подход к регулированию технологий двойного назначения — будь то запуск космического корабля или ракеты либо использование атомных реакторов для нужд энергетики или для производства расщепляющего материала — не дает применимых на практике инструментов. В отличие от боевого танка или баллистической ракеты, ни один цифровой инструмент не может считаться оружием в отрыве от обстоятельств его применения<sup>16</sup>. Подобные инструменты могут без конца воспроизводиться, переориентироваться и соединяться с физическими системами. Нет никакого отдельного набора «процессов», например двух способов обогащения и переработки в целях производства расщепляющего материала для ядерного оружия, или легко определяемых уязвимых мест, таких как выделение плутония из отработанного топлива, которые можно было бы контролировать<sup>17</sup>. С точки зрения последствий часто бывает сложно определить границу перехода от виртуального к физическому, от слежки и причинения беспокойства к межгосударственному конфликту, и от местного и национального уровня к международному. В отличие от физических боеприпасов, кибернетическое оружие не самоуничтожается и может

13 Например, в рамках заключенного в 1992 году Договора по открытому небу проводятся воздушные инспекции для проверки фактов развертывания сил с целью исключить неожиданные нападения. Arms Control Association, “The Open Skies Treaty at a Glance”, fact sheet, доступно по адресу: [www.armscontrol.org/factsheets/openskies](http://www.armscontrol.org/factsheets/openskies).

14 См. разделы MTCR Guidelines («Руководящие принципы РКРТ») и MTCR Annex («Приложение РКРТ») на веб-сайте Режимы контроля за ракетными технологиями, доступно по адресу: <https://mtcr.info> (на англ. яз.).

15 Colin Picker, “A View from 40,000 Feet: International Law and the Invisible Hand of Technology”, *Cardozo Law Review*, Vol. 23, 2001, p. 149.

16 Взять, к примеру, вредоносные программы: правоохранительные органы могут использовать те же строки кода для ведения наблюдения за террористами и создания помех для планирования терактов.

17 Зависимость от финансирования научно-исследовательских и опытно-конструкторских работ (НИОКР), определенных видов массивов данных или вычислительной мощности теоретически может считаться уязвимым местом разработки смертоносного автономного оружия, однако практических способов, позволяющих предотвратить использование всех этих инструментов для военных целей, предусмотреть невозможно.

повторно использоваться для нападения на нападающего<sup>18</sup>. Действующих лиц тоже сложно разделить на государственных и негосударственных, поскольку государства редко официально принимают на себя ответственность за кибератаки. Кроме того, сама по себе категория государственных субъектов довольно подвижна — в этой сфере нет привилегированной и статичной группы обладателей кибероружия с высоким порогом входа<sup>19</sup>. Понятия паритета и баланса, столь любезные сердцу практикующих специалистов в сфере контроля вооружений эпохи холодной войны, в цифровой среде тоже с трудом поддаются определению<sup>20</sup>.

На более базовом уровне скорость и распространенность разработки цифровых технологий превышают возможности политических форумов, не успевающих отслеживать социальные, экономические и политические последствия научно-технического прогресса<sup>21</sup>. Эта проблема еще сильнее усугубляется тем, что частный сектор сейчас играет гораздо более значительную роль в разработке новейших технологий и способов их применения в бизнесе и в создании интеллектуальной собственности по сравнению с государственным сектором<sup>22</sup>. В Таблице 1 изложены некоторые характеристики традиционных многосторонних форумов, которые осложняют работу с политическими последствиями развития цифровых технологий.

18 Примером может служить вредоносное программное обеспечение NotPetya, основанное на средстве проникновения под названием EternalBlue, которое, предположительно, было разработано Агентством национальной безопасности США, а в начале 2017 г. украдено в результате утечки информации. David Bisson, “NotPetya: Timeline of a Ransomware”, *Tripwire*, 28 June 2017.

19 В отличие, например, от Договора о нераспространении ядерного оружия, в котором каждое из пяти государств, которые произвели и взорвали ядерное взрывное устройство до 1967 г., было названо «государством, обладающим ядерным оружием» (ст. IX, п. 3).

20 В случае ядерного оружия и средств его доставки можно построить сложные модели, основанные на паритете, стабильности и балансе, поскольку их воздействие поддается изучению, а потенциал может быть оценен, рассчитан и даже закреплён в договорных системах, таких как договоры о контроле стратегических вооружений между СССР и США. Однако кибернетический потенциал — весьма запутанная сфера. В отрыве от контекста воздействие кибернетического оружия сложно не только сопоставить, но даже оценить.

21 Иллюстрацией этого сумасшедшего темпа может служить так называемый закон Мура, который гласит, что количество транзисторов, размещаемых на кристалле интегральной схемы, удваивается каждый год, причем их стоимость сокращается.

22 В Докладе о цифровой экономике за 2019 г., подготовленном Конференцией Организации Объединенных Наций по торговле и развитию (ЮНКТАД), представлен отличный анализ политических трудностей, с которыми сталкиваются традиционные форумы в сфере антимонопольной политики и правил ведения торговли в результате взрывного роста цифровой экономики. UNCTAD, *Digital Economy Report 2019*, Geneva, 2019, доступно по адресу: [https://unctad.org/en/PublicationsLibrary/der2019\\_en.pdf](https://unctad.org/en/PublicationsLibrary/der2019_en.pdf).



Таблица 1. Характеристики многосторонних форумов, которые создают сложности в отношении вопросов, связанных с цифровыми технологиями

Характеристики	Сложности
Периодичность, время реагирования	Многосторонние форумы собираются регулярно, с определенной периодичностью — часто раз в год, — хотя между заседаниями могут проводиться встречи рабочих групп и организационных комитетов. Заседания продолжаются недолго — от нескольких дней до нескольких недель. Переговоры по поводу заключения договоров занимают много лет, а конференции по обзору договоров часто созываются раз в пять лет. В цифровой сфере разработка и внедрение технологий за год могут шагнуть далеко вперед, и нерегулярных кратких заседаний недостаточно для изучения их воздействия и планирования ответных политических мер <sup>23</sup> .
Заданная повестка дня	Многосторонние форумы опираются на структурированную повестку дня и программу межсессионной деятельности в соответствии с согласованным мандатом. Вопросы, связанные с технологиями, часто рассматриваются в рамках таких обширных разделов, как «Научно-технический прогресс» или «Воздействие новых технологий». Проблемы цифровых технологий не так-то просто вместишь в статичные повестки дня и мандаты; как следует из примера Cambridge Analytica, для четкого осознания вопросов, связанных с управлением технологиями, необходима конкретика в отношении обстоятельств их применения <sup>24</sup> .

Продолжение на следующей странице

23 Примером того, как отстает не только выработка политики от развития цифровых технологий, но и понимание со стороны разработчиков политики — от быстро меняющихся технологичных бизнес-моделей и от тех, кто создает такие компании и управляет ими, могут служить показания Марка Цукерберга в Конгрессе США. Casey Newton, “The 5 Biggest Takeaways from Mark Zuckerberg’s Appearance before the Senate”, *The Verge*, 10 April 2018, доступно по адресу: [www.theverge.com/2018/4/10/17222444/mark-zuckerberg-senatehearing-highlights-cambridge-analytica](http://www.theverge.com/2018/4/10/17222444/mark-zuckerberg-senatehearing-highlights-cambridge-analytica).

24 Ibid.

Таблица 1. *Продолжение*

Характеристики	Сложности
Акцент на государства	<p>Многосторонние форумы строятся вокруг государств, а состав их участников обычно ограничен дипломатическими представителями. Для большинства делегаций межминистерское взаимодействие в преддверии многосторонних заседаний и межведомственный состав участников являются непозволительной роскошью<sup>25</sup>. Цифровые технологии обычно разрабатываются в частном секторе, и это сказывается и на уровне их понимания, и на степени их контроля со стороны государств. Кроме того, регулированием цифровых технологий часто занимаются несколько разных министерств и ведомств, что затрудняет координацию<sup>26</sup>.</p>
Осязаемость	<p>Многосторонние форумы в сфере контроля вооружений и урегулирования конфликтов ориентируются на материальное оружие и инструменты, конкретные способы производства, а также четко определенную отраслевую принадлежность и бизнес-модели. Их воздействие тоже оценивается с точки зрения осязаемых последствий — порчи имущества, причинения смерти, нанесения ущерба окружающей среде и так далее. Цифровые технологии неосязаемы; они могут не входить в состав вооружений, но при этом оказывать значительное влияние на развитие конфликта (например, через системы поддержки принятия решений), и их нельзя отделить от других технологических сфер.</p>

25 “Small Developing Countries Struggle in WTO”, *Forbes*, 19 May 2010.

26 Например, в отличие от традиционной банковской деятельности, которая регулируется министерством финансов, электронные платежи затрагивают сферу полномочий министерств финансов, связи и ИКТ.

Итоги

В отличие от других видов вооружений, цифровые технологии могут оказывать преимущественно (но не всегда исключительно) социально-психологическое воздействие, не неся в себе угрозы физического уничтожения. Это их свойство может дезориентировать практикующих специалистов, привыкших считать, сравнивать и контролировать отдельные виды вооружений и платформ.

По итогам таких форумов принимаются либо юридически обязывающие договоры, «жесткое право», которое может исполняться государствами через внутреннее законодательство и/или регламенты, либо отчеты и резолюции, которые имеют политическое влияние в рамках межгосударственных отношений. Соблюдение договоров обеспечивается посредством контрольного режима с проведением инспекций, заявлений и инспекций по запросу. Политические обязательства исполняются за счет диалога, дипломатической работы, взаимных уступок и угрозы последствий для репутации. «Жесткое право» применяется лишь в узком аспекте цифровых технологий, преимущественно в виде регулирования коммерческой деятельности, защиты потребителей и работников и так далее. Но в большинстве случаев цифровые технологии регулируются с помощью «мягкого права», в том числе «добровольных программ, стандартов, кодексов поведения, передового опыта, программ сертификации, руководств и заявлений о принципах»<sup>27</sup>. Для контроля соблюдения этих норм инспекции на местах обычно не применяются.

*Продолжение на следующей странице*

27 Wendell Wallach and Gary Marchant, “Toward the Agile and Comprehensive International Governance of AI and Robotics”, *Proceedings of the IEEE*, Vol. 107, No. 3, 2019.

Таблица 1. *Продолжение*

Характеристики	Сложности
Междисциплинарный характер	<p>По самой своей задумке и принципам работы многосторонние форумы склоняются к специальному исследованию отдельных тем (торговли, разоружения, прав человека, экологии и так далее) вне зависимости от технологий. Эта ситуация уже меняется<sup>28</sup>, но большинство участников таких форумов и соответствующих секретариатов тоже, как правило, представляют специальные области знаний. Отсутствие междисциплинарного подхода особенно очевидно на примере форумов по контролю вооружений и разоружению, участники которых обычно не взаимодействуют с разработчиками технологий и предпринимателями<sup>29</sup>. В свою очередь, разработчики технологий и предприниматели часто не осознают последствий созданных ими новшеств с точки зрения политики и безопасности. Возможности для их взаимодействия с разработчиками политики ограничены контекстом регулирования рынка, хотя в последние годы такие многосторонние мероприятия, как Всемирный экономический форум, стали расширять этот круг.</p>
Расстановка сил	<p>Многосторонние форумы функционируют на основе традиционной расстановки сил — крупные державы часто выступают как «предприниматели норм»<sup>30</sup>, а объединения государств действуют в качестве инициативных групп.</p>

28 В качестве организационных принципов в рамках недавних инициатив в сфере цифрового сотрудничества и управления интернет-пространством стали использоваться цифровые технологии и междисциплинарный характер воздействия, а не определенные ООН сферы, такие как права человека.

29 Исходя из опыта участия автора в переговорах в рамках Конференции по разоружению и в прениях в составе Комиссии ООН по разоружению с 2010 по 2017 г., взаимодействие с представителями соответствующей отрасли отсутствовало во всех случаях, в отличие от Саммита по ядерной безопасности, организованного вне рамок ООН. В контексте Конвенции о запрещении или ограничении применения конкретных видов обычного оружия взаимодействие с представителями отрасли осуществлялось в ходе мероприятий на полях в 2017–2018 гг.

30 Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change”, *International Organization*, Vol. 52, No. 4, 1998.

Хотя частные компании и представители гражданского общества сыграли важную роль в определении повестки дня и формировании мнения по итогам некоторых дискуссий<sup>31</sup>, они уступают первое место более могущественным государственным и внутригосударственным деятелям. Это асимметричное распределение сил плохо вяжется с цифровой действительностью. Например, у таких цифровых платформ, как Facebook, Alipay и WhatsApp, бывает больше пользователей («виртуальных граждан»), чем жителей в большинстве стран; они эксплуатируют практически глобальную инфраструктуру, выступают в качестве трансграничных «блюстителей контента» и далеко опережают другие отрасли по объему рыночной капитализации, по сравнению с которой ВВП большинства государств кажется ничтожно малым. Для того чтобы нормы, связанные с цифровыми технологиями, могли на что-то влиять, представители цифровой индустрии должны участвовать в обсуждении ответных политических мер и сотрудничать с государством в целях их реализации.

На фоне этих трудностей полезно рассмотреть несколько многосторонних форумов на стыке цифровых технологий и международной безопасности.

### **Отдельные многосторонние форумы, которые занимаются влиянием цифровых технологий на международную безопасность: ГПЭ ООН и Рабочая группа открытого состава по информационной безопасности**

По инициативе Российской Федерации в повестку дня Генеральной Ассамблеи ООН в 1998 году был внесен пункт «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Резолюциями Первого комитета Генеральной Ассамблеи по данному пун-

31 Можно привести два примера: Конвенция о запрещении противопехотных мин 1997 г. (Оттавская конвенция) и Договор о запрещении ядерного оружия 2017 г. Роль гражданского общества в заключении этих договоров была отмечена присуждением Нобелевской премии мира Джоди Уильямс и Международному движению за запрещение противопехотных мин в 1997 г. и Международной кампании за ликвидацию ядерного оружия в 2017 г.

кту за несколько лет было создано пять ГПЭ для изучения вопроса и формулировки рекомендаций. На данный момент действует шестая ГПЭ под председательством Гильерме Патриоты (Бразилия), а также Рабочая группа открытого состава (РГОС) по тому же вопросу под председательством посла Швейцарии Юрга Лаубера<sup>32</sup>. ГПЭ имеют ограниченный состав — от 15 до 25 назначенных правительствами экспертов — и заседают поочередно в Женеве и Нью-Йорке, а заседания РГОС открыты для всех государств — членов ООН и наблюдателей и проходят в Нью-Йорке. Ценность работы РГОС и ГПЭ ООН заключается в поддержании диалога для выработки общего понимания последствий применения цифровых технологий с точки зрения безопасности, а также в содействии внедрению норм, правил и принципов ответственного поведения государств в этой сфере. В рамках резолюций об их учреждении были предусмотрены возможности взаимодействия представителей отрасли, научных кругов и гражданского общества с этими форумами, хотя они и носят ограниченный характер (например, в форме письменных заявлений или кратких выступлений в ходе пленарных заседаний)<sup>33</sup>.

В докладе ГПЭ ООН за 2013 год отмечается, что международное право, в частности Устав ООН, применимо и важно для поддержания мира и стабильности и для содействия обеспечению открытой, безопасной, мирной и доступной среды информационно-коммуникационных технологий (ИКТ). В 2015 году ГПЭ, приняв к сведению предложенные Правила поведения в области обеспечения международной информационной безопасности, также предложила государствам комплекс из 11 добровольных и необязательных норм, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды<sup>34</sup>. Эти нормы включают в себя (добровольное) обязательство не осуществлять и заведомо не поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит обязательствам государства по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения<sup>35</sup>. Кроме того, в них

32 Новая ГПЭ была учреждена по инициативе США, тогда как Россия, прежде бывшая сторонником ГПЭ, в 2018 г. стала поддерживать методику РГОС как предполагающую более активное участие за счет открытости для всех государств-членов, однако она по-прежнему представлена в ГПЭ с ограниченным числом участников, учрежденной под эгидой США.

33 Более подробная информация о взаимодействии с различными заинтересованными сторонами и о работе с их предложениями в рамках РГОС представлена на веб-сайте Рабочей группы открытого состава, доступном по адресу: [www.un.org/disarmament/open-ended-working-group/](http://www.un.org/disarmament/open-ended-working-group/) (на англ. яз.).

34 *ГПЭ ООН*. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, док. ООН А/70/174, 22 июля 2015 г., пп. 12, 13.

35 Недавние процессы с участием многих заинтересованных сторон, такие как работа Глобальной комиссии по стабильности киберпространства (GCSC), предполагают дополнительные нормы и методы защиты, в том числе для инфраструктуры проведения выборов. GCSC, *Advancing Cyberstability: Final Report*, November 2019.

содержится запрет на нанесение ущерба группам экстренной готовности к компьютерным инцидентам других государств. Это напоминает определение охраняемых объектов/функций и принцип разграничения в рамках МГП. К сожалению, в ходе работы ГПЭ созыва 2017 года консенсус был нарушен, главным образом в связи с вопросом применимости международного права к конфликтам в киберпространстве<sup>36</sup>.

Сегодня стоит задача не только восстановить нарушенный консенсус, но и согласовать между собой результаты деятельности двух форумов, работающих параллельно над одним и тем же вопросом, — шестой ГПЭ ООН и РГОС, учрежденных в декабре 2018 года резолюциями, принятыми по инициативе США и России соответственно. Расхождения касаются не только процедуры, но и затрагивают существо вопроса: различия проходят между подходами, одна часть которых основана на применимости существующих норм к конфликтам в киберпространстве и на возможности привлечения к ответственности в рамках таких норм, а вторая часть предполагает отказ от автоматического распространения действующего международного права, в частности МГП, на конфликты в киберпространстве и подчеркивает необходимость договориться о новых нормах.

В этом отношении поучительно будет сопоставить комментарии делегатов России и США к первоначальному проекту доклада РГОС, разосланному ее председателем 11 марта 2020 года<sup>37</sup>. Представитель США внес в целом одобрительные комментарии к первоначальному проекту доклада, но выразил критику по поводу некоторых пунктов, заявив:

Мы с удовлетворением отмечаем тот факт, что в проекте доклада содержится напоминание о том, как все государства-члены вновь подтвердили: международное право и, в частности, Устав Организации Объединенных Наций применимы к использованию государствами ИКТ. <...> В настоящем проекте уделяется слишком много внимания (в пунктах 27–30) предложениям, внесенным меньшинством государств по поводу постепенного развития международного права, в том числе посредством разработки юридически обязывающего документа, регламентирующего использование государствами ИКТ. В этих предложениях отсутствует конкретика, и они не подходят для практического применения. Задача РГОС состоит в том, чтобы рассмотреть возможности применения международного права к использованию государствами ИКТ, следовательно, основное внимание в докладе должно уделяться существующему международному праву. Без четкого понимания

36 Elaine Korzak, “UN GGE on Cybersecurity: The End of an Era?”, *The Diplomat*, 31 July 2017, доступно по адресу: <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/>.

37 OEWG, “Initial ‘Pre-draft’ of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security”, 11 March 2020, доступно по адресу: <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf>.

позиций государств по поводу применимости международного права к ИКТ было бы преждевременно высказывать предположения о том, что международное право нуждается в изменениях или доработках<sup>38</sup>.

Представитель Российской Федерации отметил наличие некоторых «положительных моментов», однако упомянул о том, что в тексте содержится «множество неприемлемых для нас подходов», и заявил:

Чрезмерный акцент придается принципу применимости общепризнанных норм и принципов международного права, зафиксированных в Уставе ООН и Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом ООН 1970 г. применительно к сфере информационно-коммуникационных технологий (ИКТ). Вместе с тем отсутствует привязка данного принципа к конкретным модальностям такой применимости, а именно — кем, каким образом, в каких условиях оно применимо. Данные практические аспекты должны регламентироваться специальным универсальным международно-правовым инструментом, который урегулировал бы модальности применения существующих норм международного права в сфере использования ИКТ и предусматривал бы, при необходимости, новые нормы. <...> Потенциально опасным видится навязывание принципа полной и автоматической применимости МГП к информпространству в мирное время. Это утверждение само по себе является алогичным и противоречивым, поскольку МГП применяется только в условиях вооруженного конфликта, а на данном этапе ИКТ не подпадает под определение оружия<sup>39</sup>.

Это не единственная площадка, на которой высказываются противоположные взгляды на соотношение действующего права и новых норм. Обсуждая проблему киберпреступности, Россия, Китай и другие государства выдвинули через Генеральную Ассамблею ООН предложение провести переговоры по поводу всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях<sup>40</sup>. Многие западные страны видят в ней потенциальную угрозу правам человека и основным свободам, а также считают ее излишней с учетом наличия Конвенции о компьютерных преступлениях, приня-

38 “United States Comments on the Chair’s Pre-draft of the Report of the UN Open Ended Working Group”, доступно по адресу: <https://tinyurl.com/yyus5uv7>.

39 Комментарий Российской Федерации по первоначальному проекту доклада Рабочей группы ООН открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, доступно по адресу: <https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-rus.pdf>.

40 Резолюция Генеральной Ассамблеи ООН 74/247. Противодействие использованию информационно-коммуникационных технологий в преступных целях, проект резолюции, док. ООН A/C.3/74/L.11, 11 октября 2019 г.



той в 2001 году в Будапеште по линии Совета Европы; некоторые расценивают ее как важный шаг в будущее<sup>41</sup>.

Нынешняя геополитическая обстановка, в которой в Нью-Йорке ведется обсуждение информационной безопасности, не способствует достижению в рамках ООН договоренностей о том, что можно считать кибероружием и кибератакой в рамках действующего права о применении силы, как будут использоваться существующие нормы, регулирующие применение силы, и какие лакуны (если они имеются) необходимо заполнить с помощью дополнительных норм. Более реалистичным представляется решение вопросов о том, какие нормы применяются к конфликтам в киберпространстве и к киберпреступности и как они применяются, о привлечении к ответственности за кибератаки, о формировании взаимного доверия и наращивании потенциала, а также о развитии сотрудничества в области соблюдения норм, действующих в условиях конфликта в киберпространстве, в составе групп меньшего масштаба (так называемых «мини-сторонних» групп)<sup>42</sup>.

Значение мероприятий регионального уровня признается в резолюции, учреждающей действующую ГПЭ ООН в 2018 году, где содержится просьба к Управлению Секретариата по вопросам разоружения

поддерживать сотрудничество с такими соответствующими региональными организациями, как Африканский союз, Европейский союз, Организация американских государств, Организация по безопасности и сотрудничеству в Европе и Региональный форум Ассоциации государств Юго-Восточной Азии, для того чтобы провести заблаговременно до начала заседаний группы серию консультаций для обмена мнениями по вопросам, относящимся к мандату группы<sup>43</sup>.

41 “UN Approves Russian-Sponsored, China-Backed Bid on New Cybercrime Convention”, *South China Morning Post*, 28 December 2019, доступно по адресу: [www.scmp.com/news/world/united-states-canada/article/3043763/un-approves-russian-sponsored-china-backed-bid-new](http://www.scmp.com/news/world/united-states-canada/article/3043763/un-approves-russian-sponsored-china-backed-bid-new).

42 Например, по итогам процесса, проходившего при поддержке Киберцентра НАТО, в 2013 г. были составлены комментарии к международным нормам, известные как Таллинское руководство (в 2017 г. вышло второе издание данного документа). Составление Таллинского руководства отражает точку зрения о том, что международное право, разработанное до кибернетической эры, может применяться к кибероперациям — как проводимым государствами, так и направленным против них — и что государства при этом имеют права и обязанности в соответствии с международным правом. См.: Michael N. Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, Cambridge, 2017. Еще одним примером может служить предложение некоторыми членами Шанхайской организации сотрудничества Правил поведения в области обеспечения международной информационной безопасности. См.: Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 г. на имя Генерального секретаря, док. ООН А/69/723, 13 января 2015 г.

43 Резолюция Генеральной Ассамблеи ООН 73/266. Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности, проект резолюции, док. ООН А/С.1/73/L.37, 18 октября 2018 г., п. 4.

В рамках альтернативной резолюции по тому же пункту повестки дня, учреждающей РГОС, содержится аналогичный призыв к ООН поощрять региональные усилия, меры по укреплению доверия и повышению транспарентности, а также способствовать наращиванию потенциала и распространению передового опыта<sup>44</sup>.

Менее очевидно то, в какой степени процессы в рамках ООН могут предусматривать сотрудничество с частным сектором, который зачастую первым реагирует на кибератаки или является невольным их пособником и который сам заинтересован в устранении двусмысленности в отношении применения норм<sup>45</sup>. Участие частного сектора могло бы также сыграть важную роль в предотвращении непреднамеренной эскалации в результате ответа на кибератаки со стороны частного сектора из другой юрисдикции<sup>46</sup>. Однако по понятным причинам форумы ООН не могут поставить представителей частного сектора в один ряд с представителями государств-членов, а иногда и вовсе исключают частные компании из числа участников. Добровольные негосударственные инициативы, такие как «Парижский призыв» и Глобальная комиссия по стабильности киберпространства (GCSC), не удовлетворенные результатами работы многосторонних форумов, стали принимать меры к созданию общих знаменателей для различных заинтересованных лиц по вопросу приемлемого поведения. Подобные инициативы могут дополнять работу многосторонних межгосударственных форумов<sup>47</sup>. В последние годы Секретариат ООН и учреждения ООН также выступили с инициативой более активного привлечения частного сектора к обсуждению вопросов, связанных с технологиями. В качестве примеров можно привести ежегодный Всемирный саммит «Искусственный интеллект во благо», организуемый Международным союзом электросвязи (МСЭ), и Группу высокого уровня по цифровому сотрудничеству при Генеральном секретаре ООН.

Итак, в последние пару лет, несмотря на сложную геополитическую обстановку, сконцентрированные вокруг Нью-Йорка действия, связанные с конфликтами в киберпространстве, приняли более целенаправленный и желательный оборот. Сохраняются сложности в части взаимодействия с непривычными разработчиками норм, отсутствия возможностей выработки норм снизу вверх и необходимости деполитизировать относительно

44 Резолюция Генеральной Ассамблеи ООН 73/27. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности, проект резолюции, док. ООН A/C.1/73/L.27/Rev.1, 29 октября 2018 г., п. 11 преамбулы.

45 Технические компании на повседневной основе отражают миллионы попыток нарушить меры кибербезопасности. С их серверов могут без их ведома распространяться вредоносные программы, а потери в результате взлома или невыплаты страховой суммы из-за неоднозначности источника атак могут парализовать их деятельность.

46 Подобные предложения вносили эксперты из Франции и Индии, заседавшие в составе ГПЭ в 2017 г. Источник: личная беседа с автором.

47 Так, в итоговом докладе GCSC содержится комплекс из восьми норм, дополняющий нормы, предложенные ГПЭ в 2015 г., причем эти предлагаемые нормы распространяются как на государства, так и на негосударственных субъектов. GCSC (примечание 35 выше).

менее противоречивые аспекты конфликтов в киберпространстве, такие как оценка, оказание помощи и сотрудничество.

В Женеве особое внимание традиционно уделяется глубокому изучению вопросов экспертами в целях формулирования юридически обязывающих норм в сфере разоружения, контроля вооружений, прав человека и МПП. В этом городе, где проводится «единственный» многосторонний переговорный форум для выработки соглашений по разоружению — Конференция по разоружению<sup>48</sup>, — также располагаются штаб-квартиры Международного Комитета Красного Креста (МККК) и нескольких других организаций, в том числе Всемирной организации интеллектуальной собственности и Международного союза электросвязи (МСЭ), который играет важную роль в разработке стандартов в сфере цифровых технологий и в наращивании потенциала обеспечения кибербезопасности. Известный нейтралитет Женевы является важным соображением для многосторонних и проводимых с участием разных заинтересованных сторон мероприятий по теме кибербезопасности, поэтому неудивительно, что Институт ООН по исследованию проблем разоружения (ЮНИДИР) проводит свою ежегодную конференцию по стабильности киберпространства именно в Женеве и что этот город выбрал для своей штаб-квартиры Институт кибермира, цель которого состоит в оказании помощи жертвам кибератак и в привлечении виновных к ответственности<sup>49</sup>. Обширная экосистема гуманитарных и правозащитных механизмов, а также институтов торговли и развития в Женеве является важным активом для международного сотрудничества в области регулирования цифровой сферы, в которой не соблюдаются традиционные границы между тремя основными направлениями работы ООН: торговлей и развитием, миром и безопасностью и правами человека и гуманитарной деятельностью.

В своей статье, опубликованной в 2014 году, Джозеф Най подробно описал «комплекс режимов управления деятельностью в глобальном киберпространстве», исключив из него то, что многим представлялось неким малоизвестным форумом в Женеве на стыке МПП и контроля вооружений<sup>50</sup>. Речь идет о Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие (Конвенция по конкретным видам обычного оружия, или КОО). Конвенция, согласованная под эгидой ООН в 1979–1980 годах, опирается на ключевые принципы МПП, такие как принципы соразмерности и разграничения между гражданским населением и комбатантами. На данный момент к Конвенции

48 По итогам первой специальной сессии Генеральной Ассамблеи ООН по разоружению в 1978 г. была создана «триада» форумов по разоружению: Первый комитет Генеральной Ассамблеи ООН в Нью-Йорке, Комиссия ООН по разоружению (тоже в Нью-Йорке) как всеобщий совещательный орган и Конференция по разоружению в Женеве как «единственный» многосторонний переговорный форум для выработки соглашений по разоружению.

49 Информация об Институте кибермира доступна по адресу: <https://cyberpeaceinstitute.org/>.

50 Joseph S. Nye Jr., *The Regime Complex for Managing Global Cyber Activities*, Global Commission on Internet Governance Paper Series No. 1, May 2014.

прилагается пять протоколов: Протокол I о необнаруживаемых осколках, Протокол II о запрещении или ограничении применения мин, мин-ловушек и других устройств (в редакции от 3 мая 1996 года), Протокол III о запрещении или ограничении применения зажигательного оружия, Протокол IV об ослепляющем лазерном оружии и Протокол V по взрывоопасным пережиткам войны, в котором освещается проблема неразорвавшихся и брошенных снарядов. Модульный характер Конвенции позволяет дополнять рамочный договор новыми инструментами по мере развития технологий и возникновения новых гуманитарных проблем<sup>51</sup>.

В начале 2014 года сложно было себе представить, что Конвенция по конкретным видам обычного оружия, которая до тех пор имела дело преимущественно с системами вооружений, датировавшимися чуть ли не XIX веком, станет передовой площадкой для обсуждения вопросов влияния новых цифровых технологий на международную безопасность и международное право<sup>52</sup>. На фоне таких происшествий, как поражение вирусом Stuxnet газовых центрифуг на иранских уранообогащительных комбинатах, основное внимание уделяется вредоносному программному обеспечению и конфликтам в киберпространстве. Ряд прорывов в области машинного обучения, совершенных в 2010-х годах, вывел на передний план новый комплекс цифровых технологий, известный под общим названием «искусственный интеллект» (ИИ), в результате чего Конвенция превратилась в площадку для обсуждения смертоносных автономных систем вооружений, основанных на ИИ.

## **Регулирование автономности смертоносных функций в системах вооружений: пример Конвенции по конкретным видам обычного оружия**

Важный вклад в обсуждения в рамках Конвенции внес доклад Специального докладчика ООН по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях Кристофа Хейнса за 2013 год. Специальные докладчики — независимые эксперты в области прав человека, обладающие значительной самостоятельностью в исполнении своих мандатов и имеющие возможность запрашивать фактические данные и выражение мнения у правительств, гражданского общества, представителей научных кругов и различных отраслей<sup>53</sup>. Хейнс был обеспокоен произволом, связанным с применением беспилотных летательных аппаратов в отношении негосударственных субъектов, и риском усугубления этой проблемы при использовании технологий автономности.

51 Подробнее о Конвенции и протоколах к ней см.: UN Geneva, “The Convention on Certain Conventional Weapons”, доступно по адресу: <https://tinyurl.com/y4orq8q5>.

52 А. С. Гилл (примечание 5 выше).

53 Управление Верховного комиссара ООН по правам человека. Специальные процедуры Совета по правам человека, доступно по адресу: <https://www.ohchr.org/RU/HRBodies/SP/Pages/Welcomepage.aspx>.

Он определил смертоносные автономные роботизированные системы как «системы оружия, которые после их приведения в действие могут выби- рать и поражать цели без последующего вмешательства со стороны опе- ратора» и выразил беспокойство по поводу невозможности привлечения таких систем к ответственности и по поводу их соответствия требованиям МГП и стандартов, обеспечивающих защиту жизни человека согласно нормам международного права прав человека<sup>54</sup>. Доклад вызвал значитель- ные споры, но, поскольку было сочтено, что данная тема относится скорее к контролю вооружений и праву вооруженных конфликтов, нежели к пра- вам человека, в 2014 году под давлением ключевых делегаций в Женеве она была передана на рассмотрение в рамках Конвенции по конкретным видам обычного оружия<sup>55</sup>. В период с 2014 по 2016 год был проведен ряд нефор- мальных экспертных совещаний, благодаря которым в декабре 2016 года был достигнут консенсус об учреждении официальной ГПЭ. ГПЭ КОО — экспертный вспомогательный орган Конвенции, который уполномочен не только изучать вопросы, — как ГПЭ, учрежденные Первым комитетом в Нью-Йорке, — но и вести переговоры по поводу новых протоколов при наличии соответствующей договоренности<sup>56</sup>. Таким образом, ГПЭ КОО и другие ГПЭ, учрежденные в рамках Конвенции, отличаются от ГПЭ, учре- жденных Первым комитетом, по характеру и уровню участия тем, что они открыты для всех высоких договаривающихся сторон Конвенции. В дека- бре 2016 года в рамках Конвенции была создана новая ГПЭ — ГПЭ КОО по САС, которой высокие договаривающиеся стороны поручили изучить «новые технологии, связанные со смертоносными автономными системами вооружений»<sup>57</sup>.

Так появился форум, имеющий мандат в данной сфере и обладаю- щий некоторыми качествами, позволяющими уменьшить влияние вышепе- речисленных проблем. Его модульный характер и наличествующий прак- тический опыт дали возможность перейти от обсуждений к переговорам в отношении обязывающего инструмента. Отметим, что ГПЭ, учрежденные Первым комитетом, не располагают такими полномочиями, хотя РГОС могут переходить от обсуждений к переговорам при обновлении мандата<sup>58</sup>. Все страны, в которых развивается потенциал, связанный с системами ИИ, такие как Австралия, Бразилия, Германия, Израиль, Индия, Канада, Китай, Республика Корея, Россия, Соединенное Королевство, США, Франция, ЮАР

54 Хейнс, Кристоф. Доклад Специального докладчика по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях, док. ООН А/НRC/23/47, 9 апреля 2013 г.

55 Неудивительно, что данные делегации представляли основных владельцев и пользователей дронов, оснащенных оружием. Источник: личная беседа с автором.

56 См. справку о переговорной деятельности ГПЭ по кассетным боеприпасам в 2011 г.: UN Geneva, “GGE Sessions in 2011”, доступно по адресу: <https://bit.ly/2ZozQMI>.

57 Решение I Шестой конференции Высоких Договаривающихся Сторон по обзору Конвенции по конкретным видам обычного оружия, 12–16 декабря 2016 г.

58 Особенно ярко это проявилось в Договоре о торговле оружием, который был принят в 2013 г. по итогам процесса, продолжавшегося семь лет. Michael Spies, “Towards a Negotiating Mandate for an Arms Trade Treaty”, *Disarmament Diplomacy*, No. 91, Summer 2009.

и Япония, являются сторонами Конвенции по конкретным видам обычного оружия. Кроме того, присущий Конвенции и основным положениям МГП баланс между гуманитарными принципами и военной необходимостью дал возможность государствам с очень разными позициями начать взаимодействие по поводу сложной и стремительно развивающейся технологии.

Это не значит, что выбор площадки или продолжение ее использования для решения вопроса автономности смертоносного оружия не сопряжены ни с какими проблемами. Заседания на этой площадке проводятся на ежегодной основе, и на обсуждение выделяется одна-две недели в год<sup>59</sup>. Несмотря на то что правилами допускается участие представителей научных кругов, гражданского общества и гуманитарных организаций, заседания Конвенции по-прежнему ориентированы на государства. Таким образом, непосредственное участие разработчиков технологий на основе ИИ и представителей соответствующей отрасли в выработке правил невозможно. Кроме того, хотя выстраивание дискуссии вокруг МГП успокаивающе действует на ключевые заинтересованные стороны, тех, кто рассматривает этот вопрос преимущественно с точки зрения прав человека, это беспокоит<sup>60</sup>.

Проблема междисциплинарности была до некоторой степени решена за счет проведения мероприятий «на полях», организованных МККК, НПО, научными кругами и правительствами, которые позволили посмотреть на вопросы свежим взглядом, в том числе со стороны предпринимателей<sup>61</sup>. Обсуждения в 2017 году были построены на повышении осведомленности о технологии, отделении здравых суждений от эйфорических и антиутопических вымыслов, вычленении связей между различными сферами, объединении юридических, этических, военных и коммерческих точек зрения, а также на выходе за пределы бинарного мышления категориями гражданских и военных объектов и технологий двойного назначения<sup>62</sup>. Работа дискуссионной группы по этическому аспекту стала особенно

59 В 2017 г. ГПЭ КОО по САС заседала в течение недели, состоявшей из пяти рабочих дней; в 2018 г. продолжительность заседания выросла до десяти рабочих дней в течение двух недель, а в 2019 г. составила семь рабочих дней. В 2020 г. заседания вернулись в двухнедельный формат, тогда как в 2021 г. выделенное время позволяет заседать вплоть до четырех недель. Время, выделяемое на заседания, устанавливается в рамках ежегодного обсуждения мандата ГПЭ и зависит от бюджетных и политических соображений. В 2017 г. продолжительность заседаний была сокращена вследствие задержки выплат взносов высокими договаривающимися сторонами. См. записи мероприятий на портале UN Digital Recordings Portal, доступном по адресу: <https://conf.unog.ch/digitalrecordings/>; КОО. Совещание Высоких Договаривающихся Сторон Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезвычайные повреждения или имеющими неизбирательное действие. Заключительный доклад. Док. ООН CCW/MSP/2019/9, 13 декабря 2019 г.

60 Этой позиции придерживались многие делегации, в том числе представители Сьерра-Леоне, Коста-Рики, Мексики, Ватикана и Гондураса. Например, в ходе заседания ГПЭ КОО по САС, состоявшегося 13–17 ноября 2017 г., посол Сьерра-Леоне Иветт Стивенс заявила, что параллельно с обсуждениями этим вопросом должен продолжать заниматься Совет по правам человека.

61 См., например, программу мероприятий «на полях» заседания ГПЭ КОО по САС в 2017 г.

62 ГПЭ КОО. Документ «Пища для размышлений», док. ООН CCW/GGE.1/2017/WP.1, 4 сентября 2017 г. См. также: ГПЭ КОО. Предварительная программа работы, док. ООН, CCW/GGE.1/2017/2, 4 сентября 2017 г., в которую был включен междисциплинарный аспект за счет организации обсуждения в четырех дискуссионных группах.

полезна за счет привлечения к диалогу правозащитных и религиозных сообществ<sup>63</sup>. В том, что касается осязаемости, свидетельства и доклады независимых экспертов, исследовательских центров и таких организаций, как МККК, ЮНИДИП и SIPRI, а также рабочие документы, представленные наиболее активными делегациями, способствовали повышению осведомленности о характере технологий автономности. В организованных МСЭ саммитах «Искусственный интеллект во благо», которые, кстати, начали проходить в 2017 году через дорогу от Дворца Наций, участвовало много делегаций из разных стран, что позволило обеспечить обмен мнениями по поводу управления в сфере ИИ<sup>64</sup>.

Каковы же были результаты его деятельности? В 2017 году ГПЭ КОО по САС приняла на основе консенсуса ряд выводов и рекомендаций<sup>65</sup>. Один из них заключался в том, что Конвенция является подходящим механизмом для решения указанной проблемы, еще один гласил, что МГП полностью применимо к возможной разработке и использованию САС. Это было важное заверение на начальном этапе, хотя оно не отвечало на вопрос о том, требуются ли дополнительные юридические нормы. В выводах, принятых на основе консенсуса, также подчеркивались три проблемы для дальнейшей работы: описание рассматриваемых систем (так называемый вопрос определения), выявление аспектов взаимодействия «человек — машина», имеющих критическое значение для риска возможных нарушений МГП, а также наличие возможностей по устранению последствий применения таких систем для гуманитарной обстановки и международной безопасности. К единому мнению по поводу определений, риска и возможной пользы от САС — а также подходов к их регулированию и контролю, в том числе предложения о превентивном запрете, — прийти не удалось, но составленное председателем краткое резюме в итоге стало практическим инструментом, отражающим разнообразие позиций по поводу будущих результатов, но не препятствующим прогрессу по существу<sup>66</sup>.

Стоит сравнить относительную легкость, с которой была допущена применимость МГП в контексте САС, с тем, как долго и трудно продолжаются переговоры относительно кибероружия в ГПЭ ООН и РГОС. Как говорится в ответе на опасения по поводу ссылки на МГП, выраженные в 2017 году представителем Китая, Конвенция по конкретным видам обычного оружия относится к вооруженным конфликтам и смертоносному оружию, хотя некоторые делегации и МККК выступали за более широкий подход, предполагающий ее распространение на «автономные системы вооружений»<sup>67</sup>. Так, в контексте целей и задач Конвенции МГП, очевидно,

63 См. записи мероприятий на портале UN Digital Recordings Portal, доступном по адресу: <https://conf.unog.ch/digitalrecordings/>.

64 См. доклады по итогам Глобального саммита «Искусственный интеллект во благо» за 2017–2019 гг., доступные по адресу: <https://aiforgood.itu.int/reports/>.

65 CCW GGE on LAWS, *Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems*, UN Doc. CCW/GGE.1/2017/CRP.1, 20 November 2017.

66 A. S. Gill (примечание 5 выше).

67 См. записи мероприятий, состоявшихся 17 ноября 2017 г., на портале UN Digital Recordings Portal, доступном по адресу: <https://conf.unog.ch/digitalrecordings/>.

актуально независимо от позиций сторон в отношении того, нужны ли дальнейшие пояснения насчет применения принципов МПП к САС и/или необходимо ли разработать новые нормы.

Ключевым понятием при обсуждении САС в 2017 году является существенный контроль со стороны человека<sup>68</sup>. Это понятие привлекательно с концептуальной точки зрения, поскольку дает возможность избежать переговоров по поводу дополнительных норм для обеспечения соответствия МПП, однако по той же причине оно было сочтено проблематичным и даже поддающимся различным трактовкам. На заседании ГПЭ КОО по САС в апреле 2018 года появилась возможность рассмотреть более широкое понятие участия и вмешательства человека с точки зрения различных этапов цикла разработки технологии. Это позволило ГПЭ пойти дальше обсуждения концепции «существенного контроля со стороны человека» или подобных понятий вроде «надлежащего человеческого суждения» и изучить качество и глубину взаимодействия «человек — машина», необходимого для соблюдения МПП по существу на каждом из этапов разработки, развертывания и применения технологии. Кроме того, благодаря этому появился выбор стратегий управления на разных уровнях для обеспечения более четкой ответственности и подотчетности человека. Полукруговая диаграмма, изображенная на рисунке 1, резюмирует результаты этой дискуссии и демонстрирует распределенную схему управления технологией, которая учитывает международные нормы, подходы к регулированию в различных странах и стандарты саморегулирования отрасли<sup>69</sup>.

Ранее мы видели, как отсутствие согласованного определения кибероружия стало препятствием к достижению результатов в области юридических норм. Проблема определения САС тоже могла бы застопорить всю работу в рамках Конвенции по конкретным видам обычного оружия, но она была отложена для пошагового изучения. На своем заседании в апреле 2018 года ГПЭ КОО по САС использовала «принцип Lego», собирая различные характеристики, которые могут потребоваться для описания САС, но не выбирая из них поначалу конкретные определения и не замыкаясь исключительно на технических свойствах. Например, попытка сформулировать определение на раннем этапе могла бы привести к тому, что в процессе разработки технологий некоторые подобные системы

68 CCW GGE, *Examination of Various Dimensions of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, in the Context of the Objectives and Purposes of the Convention: Submitted by the Netherlands*, UN Doc. CCW/GGE.1/2017/WP.2, 9 October 2017.

69 На первый взгляд может показаться, что изображенные на полукруговой диаграмме этапы НИОКР, а также тестирования и оценки исключены из сферы влияния международного регулирования. Помимо того, что степень международного регулирования еще только предстоит определить — и в этом смысле три варианта регулирования, построенные на отраслевых стандартах, государственном регулировании и международных нормах, представляют собой «раздвижные двери», — на этом рисунке не исключено проникновение международных норм во внутригосударственные режимы НИОКР, тестирования и оценки — подобно тому, как обзоры вооружений в МПП нашли свое отражение в практике отдельных стран.





Рисунок 1. Точки взаимодействия для усиления участия и надзора со стороны человека и для распределенного управления новыми технологиями в сфере смертоносных автономных систем вооружений

вооружений могли бы остаться за кадром<sup>70</sup>. Таким образом, был найден общий фундамент из концепций и характеристик, который потребуется для формулирования в конечном счете определения без поиска идеального разграничения между автономным (в будущем) и автоматизированным (в настоящем). Кроме того, было достигнуто понимание по вопросу о том, что технологии, имеющие отношение к САС, придется постоянно изучать как для понимания того, с чем имеют дело делегаты, так и для оценки их потенциального воздействия на региональную и международную безопасность<sup>71</sup>.

Важным осозаемым результатом стало принятие в августе 2018 года комплекса «Возможных руководящих принципов»<sup>72</sup>. Такой итог переговоров был бы немислим без достигнутого годом ранее консенсуса по пункту 16 доклада ГПЭ КОО по САС за ноябрь 2017 года, в котором отмечалось в качестве основополагающего принципа, что МГП по-прежнему будет полностью применяться ко всем системам вооружений, включая

70 Риск неполного охвата некоторыми определениями в ряде стран и раньше представлял проблему для ведения переговоров по разоружению и контролю вооружений, и опыт провала переговоров по поводу протокола о кассетных боеприпасах в рамках Конвенции в 2011 г. наверняка отягощал умы некоторых делегатов.

71 CCW GGE on LAWS, Report of the 2018 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, UN Doc. CCW/GGE.1/2017/CRP.3, 23 October 2018, paras 24–26.

72 Ibid., para. 21.

возможные разработки и применение САС<sup>73</sup>. Тот факт, что руководящие принципы являются не конечной точкой, а необходимой основой для будущей работы, подчеркивается и в принятом на основе консенсуса докладе за 2018 год, в котором рассматриваются четыре варианта ответных политических мер: разработка юридически обязывающего документа, предусматривающего запреты и регулирующие положения применительно к САС; принятие политической декларации, в которой подчеркивались бы необходимость человеческого контроля за применением силы и важность отчетности человека, а также элементов транспарентности и оценки технологий; определение практических мер и передовой практики для улучшения соблюдения норм международного права; и возможность «ничего не предпринимать», поскольку МПП в полной мере применимо к этой сфере<sup>74</sup>.

Десять принципов, согласованные в 2018 году, включают применимость МПП, сохранение ответственности человека, ответственность за применение силы в соответствии с нормами международного права, обзор оружия перед развертыванием, обеспечение физической защищенности, нераспространения и кибербезопасности, оценку риска и меры по его уменьшению в ходе разработки технологии, недопущение ущерба для научно-исследовательских и опытно-конструкторских работ (НИОКР) и применения технологий в гражданской сфере, необходимость отказаться от подхода к ИИ с позиций антропоморфизма и принятие КОО как надлежащей основы для рассмотрения данной проблемы<sup>75</sup>. Они сопровождаются широким пониманием интерфейса «человек — машина», вопроса возможного определения САС и постоянного обзора технологий, имеющих отношение к САС. Как показано на рисунке 1, понимание интерфейса «человек — машина» строится на точках взаимодействия — от политического указания на этапе, предшествующем разработке, вплоть до оценки по итогам применения. Важно отметить, что ГПЭ КОО по САС подтвердила: все эти разнообразные точки взаимодействия «человек — машина» в контексте Конвенции связаны подотчетностью. Кроме того, участники ГПЭ пришли к согласию по поводу необходимости идти в ногу с развитием технологий и совместно с представителями отрасли и другими заинтересованными сторонами формировать единый научно-политический язык, понятный для всех стран мира<sup>76</sup>.

По итогам сессии ГПЭ в 2019 году к вышеперечисленным десяти принципам был добавлен еще один, который опирается на ранее проведенную работу по интерфейсу «человек — машина» и по применимости МПП:

73 CCW GGE on LAWS (примечание 65 выше), para. 16(b).

74 ГПЭ КОО по САС. Доклад сессии 2018 года Группы правительственных экспертов по вопросам, касающимся новых технологий в сфере создания смертоносных автономных систем вооружений, док. ООН CCW/GGE.1/2018/3, 23 октября 2018 г.

75 Там же, раздел III.A «Возможные руководящие принципы».

76 А. С. Гилл (примечание 5 выше).

Взаимодействие человека и машины, которое может иметь различные формы и осуществляться на различных этапах жизненного цикла оружейной системы, должно обеспечивать, чтобы потенциальное применение оружейных систем, основанных на новых технологиях в сфере создания смертоносных автономных систем вооружений, соответствовало применимым нормам международного права, в частности международного гуманитарного права (МГП). При определении качества и степени взаимодействия человека и машины следует учитывать целый ряд факторов, включая оперативный контекст, а также характеристики и возможности оружейной системы в целом<sup>77</sup>.

Можно возразить, что одних лишь принципов может быть недостаточно, что они должны быть четко увязаны с практикой и с подотчетностью. Такая критика была бы справедлива, однако с учетом проблем, которые возникли в связи с необходимостью достичь консенсуса по сложному вопросу в быстро меняющейся сфере, начинать работу с формулирования принципов полезно в том плане, что такой подход позволяет со временем прийти к целому ряду договоренностей без ущерба для любого механизма, который может в итоге быть выбран для заключения международного соглашения.

### **Будущие направления развития для многосторонних форумов, посвященных кибербезопасности и автономному оружию**

Можно с большой долей уверенности сформулировать три прогноза в отношении цифровых технологий в условиях вооруженного конфликта. Под влиянием цифровых технологий прежде отделенные друг от друга сферы научно-технического прогресса продолжают сближаться, создавая новые сценарии применения технологий как в гражданской, так и в военной области<sup>78</sup>. Запретить кибероружие на законодательном уровне будет сложно; более того, спектр видов атак со стороны недобросовестных игроков будет и дальше расширяться — например, по мере активизации использования больших данных для прогнозирования в сфере охраны здоровья конкретного человека и точного определения тенденций в общественном здравоохранении<sup>79</sup>. Автономность технических систем продолжит возрастать, а ИИ станет технологией общего назначения, которая будет использоваться

77 ГПЭ КОО по САС. Доклад сессии 2019 года Группы правительственных экспертов по вопросам, касающимся новых технологий в сфере создания смертоносных автономных систем вооружений, док. ООН CCW/GGE.1/2019/3, 25 сентября 2019 г., раздел III, п. 16.

78 Поскольку сферы геномики, новых инфекционных заболеваний и цифровых технологий являются смежными, новые проблемы будут вставать и перед другими многосторонними форумами, не упомянутыми в этом исследовании, такими как Конвенция о биологическом и токсинном оружии 1972 г. Eleonore Pauwels, “The Internet of Living Things”, *Scientific American Blog*, 25 July 2017.

79 Michael Snyder and Wenyu Zhou, “Big Data and Health”, *Lancet Digital Health*, Vol. 1, 29 August 2019.

во всех сферах военной деятельности — от призыва и обучения до принятия решений о применении силы.

Какие направления развития многосторонних форумов возможны в таких условиях? Уникальность этих форумов состоит в их способности собирать участников и обеспечивать представительство всех сторон. Их конкурентным преимуществом является предоставление нейтральной площадки для проведения переговоров об общих принципах и нормах с целью прояснить, что приемлемо, а что нет. Нынешние задачи в цифровой сфере требуют от этих форумов расширения их границ и уменьшения барьеров для входа, чтобы привлечь к участию различных субъектов, в частности разработчиков технологий, представителей отрасли, научных кругов и гражданского общества, в том числе с целью сдерживания растущего технонационализма. Их секретариаты и должностные лица должны продемонстрировать творческий подход и гибкость, для того чтобы организовать взаимодействие с представителями отрасли, разработчиками технологий и гражданским обществом. В частности, для объединения всех этих столь разных субъектов необходимо вырабатывать общее представление на каждом этапе работы.

Помимо привлечения на заседания нужных специалистов, многосторонним форумам необходимо подумать об изменении своего подхода к выработке норм и определить, каким нормам важно отдать приоритет в цифровую эпоху<sup>80</sup>. Значение, которое придается сейчас международным договорам, должно сместиться; преимуществом должна пользоваться гибкая палитра юридических, политических и технических норм. Как показывает пример Конвенции по конкретным видам обычного оружия, речь не идет о взаимоисключающем выборе между общими принципами и обязательными мерами. Первые вполне могут вести к последним. В дальнейшем уже даже не обязательно применять один и тот же набор принципов к каждому вопросу, связанному с цифровыми технологиями. Форумы могут внедрить свои собственные механизмы выявления основополагающих принципов в зависимости от обстоятельств (если вспомнить формулировку из мандата ГПЭ КОО по САС — «в рамках целей и задач»), а затем подумать о том, какие подходы к реализации этих принципов целесообразны и эффективны в данных обстоятельствах<sup>81</sup>. Это даст вторую палитру мер контроля соблюдения норм и позволит согласовать действия не только между государствами, но и между отраслевыми органами, правительствами

80 Теоретический взгляд на эту проблему см. в: Eric Talbot Jensen and Ronald T. P. Alcalá (eds), *The Impact of Emerging Technologies on the Law of Armed Conflict*, Oxford University Press, New York, 2019, особенно в главе: Rebecca Crootof, “Regulating New Weapons Technology”.

81 Примером может служить недавнее принятие Министерством обороны США пяти принципов этичного развития ИИ, см.: DoD, “DoD Adopts Ethical Principles for Artificial Intelligence”, press release, 24 February 2020, доступно по адресу: [www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethicalprinciples-for-artificial-intelligence/](http://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethicalprinciples-for-artificial-intelligence/). Есть надежда, что за этим последуют конкретные меры, направленные на практическое внедрение этих принципов и поясняющие их взаимосвязь с юридическими обязательствами в отношении использования ИИ в системах вооружений.

стран и международными организациями. Это тоже не означает обязательной отмены режимов проверки на местах в тех случаях, когда последствия несоблюдения требований могут быть слишком тяжелы; речь, скорее, идет об объединении таких мер и сочетании их с обменом практическим опытом, а также с обзорами и комментариями со стороны коллег для создания нормативного давления.

Для иллюстрации вышеописанного подхода на примере Конвенции по конкретным видам обычного оружия можно принять за основные нормы 11 принципов, согласованных по итогам работы ГПЭ КОО по САС в 2017–2019 годах<sup>82</sup>. Впоследствии они могут сформировать ядро политического реагирования, в котором следует учесть три других критически важных элемента.

1. Комплекс практических знаний в области национальных механизмов обзора потенциальных автономных смертоносных систем вооружений с точки зрения соблюдения обязательств в рамках МПП и другого применимого международного права и исключения тех систем, которые не соответствуют таким обязательствам.
2. Комплекс практических знаний в области повышения качества интерфейса «человек — машина» в системах на основе ИИ, разрабатываемых и развертываемых в военной сфере. Это позволит рассмотреть несмертоносные составляющие систем, такие как системы поддержки принятия решений, которые могут влиять на масштаб и интенсивность конфликта.
3. Регулярное обсуждение вопросов, связанных с технологиями, в рамках Конвенции (не обзорный механизм), что позволит рассматривать возможное уточнение политических мер в свете будущих научно-технических достижений. В таком формате можно будет официально закрепить участие разработчиков технологий и представителей отрасли и, может быть, создать новую модель многосторонних форумов с участием этих заинтересованных сторон.

Практическое воплощение перечисленных тезисов могло бы стать прерогативой отдельных государств в соответствии с вышеупомянутой схемой распределенного управления технологиями. Тем не менее добровольный обмен опытом по поводу обзора вооружений и интерфейса «человек — машина» на базе существующей структуры в Женеве позволит создать необходимое давление со стороны коллег и способствовать более тщательной и ответственной работе на всех уровнях управления. Вся эта система может творчески опираться на механизм Конвенции по конкретным видам обычного оружия, если такое решение будет принято в ходе следующей Конференции по обзору в 2021 году.

Что можно сказать о форумах, посвященных кибербезопасности? Сейчас слишком сложно кардинально перестраивать существующие

82 См.: ГПЭ КОО по САС (примечания 74 и 77 выше).

форумы или возвращаться к только что отзвучавшим взаимным обвинениям в связи с проблемой применимости международного права, но можно расширить масштаб компромиссов посредством создания дополнительных существенных направлений работы. Наряду с выработкой основных норм в ГПЭ ООН и РГОС можно начать параллельное обсуждение характеристик и пользовательских сценариев, отслеживаемости, сотрудничества и оказания помощи. Среди тех, кто будет руководить этой работой, должны быть представители отрасли и научных кругов из различных регионов. По примеру предлагаемого механизма обсуждения технологий в контексте САС эти направления работы могут сформировать модель привлечения отраслевых специалистов и экспертов по теме к управлению цифровыми технологиями в условиях вооруженного конфликта.

Обсуждение характеристик в контексте конкретных примеров кибератак, с которыми сталкивается отрасль, — на первом этапе можно сосредоточиться на киберпреступности или вирусах-вымогателях — позволит выработать различные подходы к определениям. Кроме того, оно может помочь в выявлении обычных стандартов представления доказательств, подходов к оценке обстановки и смягчающих обстоятельств, а также критериев оценки ущерба на основе финансовых потерь или простоя критически важной информационной инфраструктуры.

Задача этого второго направления работы будет состоять в том, чтобы решить сложный вопрос, связанный с определением виновных, в духе сотрудничества и дружелюбия. На практике обсуждение можно построить вокруг создания независимых средств отслеживания и составить список экспертов, которые при помощи соответствующих выделенных правительствами и отраслью средств разработают четкие, прозрачные и приемлемые для всех стандарты и методики сбора и анализа фактических данных, связанных с происхождением и проведением нападений, а также оценки обстоятельств и ущерба, нанесенного такими нападениями<sup>83</sup>. При наличии соответствующей нормативной базы показания систем отслеживания, снятые в нейтральной и деполитизированной обстановке, должны помочь мирному разрешению споров без взаимных обвинений, устранить источники вредоносных программ, о которых государства не знали и за которые они не взяли на себя ответственность, защитить уязвимые места и содействовать урегулированию претензий, в том числе взысканию ущерба по страховкам. Формирование такого потенциала гораздо практичнее, чем создание механизма поиска виновных и обеспечения соблюдения норм, для которого у организаций в составе ООН нет необходимых ресурсов или политической поддержки.

Третье направление может заниматься разработкой методик обмена опытом на уровне стран, распространением информации и наращиванием

83 Несмотря на разницу в контекстах, отслеживаемость также будет являться важным аспектом обеспечения подотчетности применительно к САС за счет проверки на государственном или отраслевом уровне методики конструирования, данных для обучения, результатов тестирования и оценки.

потенциала через глобальные и региональные сети. Хотя киберпреступность не знает границ, защита систем до сих пор преимущественно остается прерогативой самих государств. Дефицит доверия и соперничество между культурой и регулированием еще больше осложняют обмен информацией между группами экстренной готовности к компьютерным инцидентам, правоохранительными органами и представителями отрасли. Демолитизация работы групп экстренной готовности к компьютерным инцидентам и создание инструментов поддержания доверия на основе технологий или привлечения нейтральных третьих лиц могло бы способствовать предоставлению информации об угрозах, скоординированному раскрытию сведений об уязвимых местах и совместному принятию ответных мер. При наличии соответствующей нормативной базы в рамках этого направления можно было бы также предоставлять независимый международный потенциал оказания помощи на базе списка независимых экспертов из разных географических областей, которые могли бы сами оказать поддержку или задействовать специально выделенные ресурсы государства и отрасли для предоставления помощи жертвам массированных кибератак<sup>84</sup>. Такой потенциал должен дополнять меры, принимаемые группами экстренной готовности к компьютерным инцидентам, которые первыми реагируют на атаки, и направляться на возмещение ущерба и оказание дополнительной помощи жертвам, выходя за рамки действующих полномочий национальных и региональных групп экстренной готовности к компьютерным инцидентам.

Стратегические аспекты, общие для всех трех направлений, позволяют привлечь больше участников к обсуждению вопросов, связанных с управлением, демолитизировать оценку уязвимых мест, оказание помощи и сотрудничество, а также сместить акцент с формирования норм государством сверху вниз. В свете предложенной в настоящей статье схемы всем трем направлениям присущ многоступенчатый подход к выработке норм. Стандарты разработки защищенного программного обеспечения, оценки и раскрытия уязвимых мест, отказа от нанесения ответного удара в случае кибератак и так далее могут изначально формулироваться на уровне отрасли с участием представителей государства в качестве наблюдателей. Нормы отслеживания, сотрудничества и оказания помощи могут разрабатываться совместными усилиями и внедряться через национальное законодательство, а межправительственные форумы, ориентированные на уровень государств, могут продолжать работу в области применимости международного права и разработки новых международных норм. Подобно параллельно работающим раздвижным дверям, эти три варианта регулирования в совокупности могут обеспечить гибкий ответ на проблему многостороннего управления цифровыми конфликтами, связанную со стремительным развитием цифровых технологий.

84 Такие дискуссионные группы оказались довольно успешными в других контекстах; перечень экспертов по вопросам, связанным с нападением с применением химического и биологического оружия, ведет Генеральный секретарь ООН. См.: UN Office for Disarmament Affairs, “Secretary-General’s Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons”, доступно по адресу: [www.un.org/disarmament/wmd/secretary-general-mechanism/](http://www.un.org/disarmament/wmd/secretary-general-mechanism/).

## Подведение итогов

В цифровую эпоху вооруженные конфликты принимают новые формы. Становится сложнее как выявлять виновных, так и привлекать их к ответственности, а границы между государствами, которые до сих пор составляли для многосторонних форумов основной предмет регулирования, и негосударственными субъектами размываются. Сама технология беспрестанно смещается и может быть превращена в оружие непредсказуемыми способами. Многосторонние нормы и практика их выработки должны приспособливаться к ситуации за счет повышения гибкости и эффективности. В настоящей статье изложен комплекс проблем, которые необходимо преодолеть многосторонним форумам, чтобы добиться успеха в области регулирования воздействия цифровых технологий на международную безопасность: чрезмерно структурированные повестки дня, ориентированность на государства и ограниченные варианты представления результатов. В статье рассмотрены предпринятые в последнее время попытки многостороннего регулирования существующего кибероружия и новых смертоносных автономных систем вооружений. Опираясь на опыт таких переговоров и другие тенденции, автор предложил будущее направление развития ГПЭ КОО по САС и форумов, посвященных проблеме кибероружия. Ключевыми вехами в предлагаемом на будущее режиме работы являются междисциплинарный характер работы, активное взаимодействие с представителями частного сектора, многоступенчатый подход к выработке норм, позволяющий синхронизировать международное регулирование с национальным законодательством и отраслевыми стандартами, а также модульное наращивание обязательств, предусмотренных руководящими принципами.