



Генеральная Ассамблея

Distr.: General
15 July 2021
Russian
Original: English

Семьдесят шестая сессия

Пункт 74 предварительной повестки дня*

Право народов на самоопределение

Использование наемников как средство нарушения прав человека и препятствования осуществлению права народов на самоопределение

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить Генеральной Ассамблее доклад Рабочей группы по вопросу об использовании наемников как средстве нарушения прав человека и противодействия осуществлению права народов на самоопределение в соответствии с резолюцией [75/171](#) Ассамблеи и резолюцией [42/9](#) Совета по правам человека.

* [A/76/150](#).



Доклад Рабочей группы по вопросу об использовании наемников как средства нарушения прав человека и противодействия осуществлению права народов на самоопределение

Воздействие на права человека наемников, субъектов, связанных с наемниками, и частных военных и охранных компаний, участвующих в кибердеятельности

Резюме

В настоящем докладе Рабочая группа по вопросу об использовании наемников как средства нарушения прав человека и противодействия осуществлению права народов на самоопределение рассматривает предоставление наемниками, связанными с наемниками субъектами и частными военными и охранными компаниями военной продукции и услуг по обеспечению безопасности в киберпространстве и последствия такой деятельности для прав человека.

В киберпространстве предоставляется широкий спектр услуг в области обороны и безопасности, включая сбор данных, разведку и шпионаж. Частные субъекты могут привлекаться государствами и негосударственными субъектами, устанавливающими опосредованные отношения различного характера, для проведения наступательных или оборонительных операций и для защиты собственных сетей и объектов инфраструктуры, а также для проведения киберопераций в целях ослабления военного потенциала и возможностей вооруженных сил противника или в целях подрыва целостности территории других государств. Лица, совершающие кибератаки, могут наносить ущерб на удалении, действуя через различные правовые системы. Поэтому они могут рассматриваться как лица, занимающиеся деятельностью, связанной с наемничеством, или даже наемнической деятельностью, если все соответствующие критерии соблюдены.

Настоящее тематическое исследование направлено на изучение характеристик и деятельности этих субъектов, получающих выгоду от разработки, содержания и эксплуатации кибермощностей, которые могут быть использованы для ведения враждебной деятельности как в ходе конфликта, так и в бесконфликтной обстановке. В нем анализируются последствия такой деятельности для прав человека, включая право народов на самоопределение, а также рассматривается вопрос о регулировании предоставления военной продукции и услуг по обеспечению безопасности в киберпространстве.

В ходе подготовки настоящего доклада в состав Рабочей группы входили Елена Апарац (Председатель), Лилиан Бобеа, Равиндран Даниэль, Крис Кваджа и Сорча Маклеод.

Содержание

I.	Введение и контекст	4
II.	Соображения в отношении определений	5
III.	Военные услуги и услуги по обеспечению безопасности в киберпространстве: деятельность, категории участников и отношения между государственными и негосударственными субъектами	7
A.	Категории соответствующих киберсубъектов	8
B.	Отношения между государственными и негосударственными субъектами	11
IV.	Регулирование роли и участия наемников, субъектов, связанных с наемниками, и частных военных и охранных компаний в предоставлении киберуслуг	14
A.	Устав Организации Объединенных Наций	14
B.	Международные права человека и гуманитарное право	15
C.	Международное уголовное право	17
D.	Стандарты права и текущие инициативы	18
V.	Последствия для прав человека	19
VI.	Выводы и рекомендации	22

I. Введение и контекст

1. Настоящий доклад представляется Генеральной Ассамблее Рабочей группой по вопросу об использовании наемников как средстве нарушения прав человека и противодействия осуществлению права народов на самоопределение; доклад представляется в соответствии с резолюцией 75/171 Ассамблеи и резолюцией 42/9 Совета по правам человека.
2. Во исполнение этого мандата Рабочая группа проводит мониторинг наемников и связанной с наемничеством деятельности во всех ее формах и проявлениях, а также частных военных и охранных компаний в различных частях мира. Кроме того, Рабочая группа изучает их деятельность и то влияние, которое она может оказать на права человека, включая право на самоопределение.
3. Настоящий доклад основан на обширных аналитических исследованиях и материалах, полученных от соответствующих заинтересованных сторон в ответ на призыв к представлению материалов, с которым Рабочая группа обратилась в январе 2021 года¹. 7 декабря 2020 года Рабочая группа провела онлайн-консультацию экспертов по вопросу о наемниках и связанных с ними субъектах в контексте кибербезопасности и новых технологий с целью включения ее результатов в настоящий доклад. Рабочая группа благодарит всех, кто внес свой вклад в подготовку доклада, предоставив информацию и приняв участие в консультациях с экспертами.
4. Обсуждения деятельности наемников на протяжении многих лет были сосредоточены на традиционных способах ведения войны, в которых наемники участвуют либо от имени государств, либо от имени других клиентов. В последнее время наемники, субъекты, связанные с наемниками, и частные военные и охранные компании стали действовать в киберпространстве. В своем докладе об изменяющихся формах, тенденциях и характеристиках наемников и деятельности, связанной с наемничеством (см. A/75/259), Рабочая группа упомянула так называемых «кибернаемников» как одну из категорий субъектов, которые могут порождать деятельность, связанную с наемничеством. Кроме того, вопрос об использовании технологий и передаче знаний регулярно поднимается в ежегодных докладах Рабочей группы в связи с различными темами². В настоящем докладе рассматривается предоставление военной продукции и услуг по обеспечению безопасности в киберпространстве наемниками, субъектами, связанными с наемниками, и частными военными и охранными компаниями, а также последствия такой деятельности для прав человека.
5. В своих предыдущих анализах Рабочая группа указывала на ряд наемников и связанных с наемниками субъектов, которые продолжают влиять на ход современных вооруженных конфликтов, нарушать права человека и подрывать право на самоопределение, в том числе с помощью деятельности в киберпространстве. Сегодня киберпространство представляет собой крупную геостратегическую арену для государственных и негосударственных субъектов, причем различные частные структуры мобилизуют и используют как оборонительный, так и наступательный киберпотенциал ради выполнения задач или удовлетворения интересов других лиц, что имеет пагубные последствия для осуществления прав человека и права народов на самоопределение.

¹ См. URL: www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx.

² См. A/75/259, пункт 50; A/HRC/45/9, пункт 39 и далее; A/HRC/42/42.

6. В частности, Рабочая группа ранее отмечала все более асимметричный характер современных вооруженных конфликтов, а также рост участия частных субъектов (A/75/259). Хотя традиционная кинетическая война продолжает играть важную роль в современных конфликтах, использование кибератак и других киберопераций становится все более распространенным явлением по мере разработки и развития новых технологий даже вне всякой связи с традиционными вооруженными конфликтами. Как следствие этих тенденций современные наемники и другие субъекты стали активно работать в киберпространстве и приспособляться к нему, а в некоторых случаях они стали необходимым компонентом киберопераций.

II. Соображения в отношении определений

7. Термин «наемник» определен в статье 47 Дополнительного протокола I к Женевским конвенциям 1949 года, Международной конвенции о борьбе с вербовкой, использованием, финансированием и обучением наемников и Конвенции Организации африканского единства о ликвидации наемничества в Африке. Тем не менее определение «наемник» в международном праве стало предметом многочисленных анализов и размышлений, сосредоточенных на его чрезмерно ограничительном характере. Рабочая группа признает, что сфера охвата этого определения проблематична и что заданные критерии трудно соблюсти, особенно в отношении современных форм деятельности, связанной с наемничеством, в том числе, когда эта деятельность осуществляется в киберпространстве негосударственными субъектами.

8. Кроме того, в отсутствие согласованного на международном уровне юридического определения Рабочая группа ранее определила термин «частные военные и охранные компании» как корпоративные структуры, предоставляющие платные военные и/или охранные услуги, обеспечиваемые физическими и/или юридическими лицами³. Они могут действовать как в условиях конфликта, так и в мирное время и являются крупными поставщиками военной продукции и услуг по обеспечению безопасности в киберпространстве.

9. Хотя ни одно из приведенных выше определений не содержит прямых упоминаний кибердеятельности или лиц, действующих в киберпространстве, все же ясно, что некоторые действия в киберпространстве могут достигать уровня наемничества или могут считаться деятельностью, связанной с наемничеством, а также могут влиять на права человека как в ходе вооруженного конфликта, так и в мирное время. Такие действия могут включать вредоносные кибероперации, проводимые киберпосредниками независимо от их гражданства или места их деятельности, а также от того, действуют ли они вне киберпространства или в режиме онлайн, и от того, причиняют они вред прямо или косвенно⁴. Под вредоносными кибероперациями понимается совершение преднамеренных действий и операций для изменения, нарушения работы, обмана, ухудшения или уничтожения компьютерных систем или сетей или для нарушения каким-либо иным образом конфиденциальности, целостности и доступности компьютерных систем или сетей для отдельных лиц и сообществ⁵. К ним не относятся новые технологии — например, технология беспилотников, — которые оказывают кинетическое воздействие за пределами компьютерных сетей.

³ Полное определение см. в A/HRC/15/25, приложение, статья 2.

⁴ Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018), p. 31.

⁵ Herbert S. Lin, "Offensive cyber operations and the use of force", *Journal of National Security Law and Policy*, vol. 4, No. 1 (13 August 2010), pp. 4–63; and ISO/IEC 27000:2009.

10. Однако Рабочая группа хотела бы подчеркнуть, что военные услуги и услуги по обеспечению безопасности, предоставляемые в киберпространстве, не должны рассматриваться как обозначение операций, связанных с наемничеством в целом, а каждый возможный случай из этих категорий надо анализировать с учетом его конкретных условий и обстоятельств (см. [A/75/259](#), пункт 54).

11. В 2020 году Рабочая группа признала кибервойну методом ведения войны, посредством которого можно не только проникать на военные или гражданские объекты, нарушать их функционирование, наносить им ущерб и даже уничтожать их, но и причинять огромный вред людям. Международный комитет Красного Креста пришел к выводу, что по аналогии с обычной войной она должна соответствовать положениям международного гуманитарного права⁶. Это тем более актуально, поскольку стратегические возможности все больше зависят от инфраструктуры и технологий (см. [A/75/259](#), пункт 42).

12. Чтобы пролить свет на это явление, Рабочая группа учитывала, в частности, изменение характера современных конфликтов и быстрое развитие новых форм ведения войны в сочетании с недостаточным регулированием, наблюдением и надзором, а также учитывала трудности расследования преступлений, совершаемых с пересечением различных правовых систем. Неравный доступ некоторых развитых стран и богатых субъектов к технологиям и знаниям в этой области также вызывает озабоченность у Рабочей группы.

13. Рабочая группа помнит о том, что условия, в которых действуют наемники, по-разному и неодинаково влияют на женщин, детей и другие группы (см. [A/75/259](#), пункт 5). Рабочая группа отмечает трудности, возникающие из-за отсутствия согласованного на международном уровне определения того, что представляет собой в рамках международного гуманитарного права кибератака или враждебная кибероперация, и поэтому в настоящее время трудно включить в рамки международного гуманитарного права концепцию враждебной кибердеятельности и выявить несоблюдения и нарушения этого права.

14. Важнейшим элементом продолжающихся дискуссий о том, когда, где и как регулируется и могла бы регулироваться такая кибердеятельность, является роль негосударственных субъектов в кибердеятельности и кибервойнах, в частности наемников, субъектов, связанных с наемниками, частных военных и охранных компаний, а также других частных и коммерческих структур. Поэтому Рабочая группа стремится рассмотреть в настоящем докладе ряд военных услуг и услуг по обеспечению безопасности, предоставляемых в киберпространстве, которые могут порождать деятельность, связанную с наемничеством, с тем чтобы стимулировать дискуссию о том, как лучше сформулировать и решить эти проблемы (см. [A/75/259](#), пункт 52). Для решения проблем, связанных с этим явлением, надо развивать не только регулирование, но и эффективное сотрудничество на национальном и международном уровнях между соответствующими субъектами.

⁶ Международный комитет Красного Креста, «Международное гуманитарное право и кибероперации во время вооруженных конфликтов», документ с изложением позиции МККК, ноябрь 2019 года.

III. Военные услуги и услуги по обеспечению безопасности в киберпространстве: деятельность, категории участников и отношения между государственными и негосударственными субъектами

15. Военные услуги и услуги по обеспечению безопасности включают в себя целый ряд услуг, в том числе сбор данных и шпионаж. Частные субъекты могут привлекаться государствами и негосударственными субъектами в рамках различных опосредованных отношений для проведения наступательных или оборонительных операций по защите собственных сетей и объектов инфраструктуры, а также для проведения киберопераций с целью ослабления военного потенциала и возможностей вооруженных сил противника или подрыва целостности территории другого государства. В ходе применения их наступательного или оборонительного киберпотенциала прослеживается связь этих субъектов с попытками или действиями, направленными на обнаружение, инфильтрацию и дезорганизацию важнейших военных или гражданских объектов с целью их уничтожения.

16. Как упоминалось выше, важно отметить, что киберуслуги предоставляются государствам вне всякой связи с вооруженными конфликтами, в том числе не только для сбора разведанных и наблюдения, но и для обеспечения правопорядка и безопасности внутри страны⁷. Кроме того, киберуслуги включают как оказание государствам услуг по поддержке существующего киберпотенциала, так и предоставление киберпродукции, которую могут использовать государства. Важно отметить, что огромный спектр продукции и услуг предоставляется и доступен для приобретения на открытом рынке, и это надо учитывать при рассмотрении вопроса о регулировании киберуслуг.

17. Многочисленные виды кибердеятельности и методы киберопераций, которые применяются в настоящее время, включают, в частности, саботаж с использованием вредоносных программ и вирусов-вымогателей, шпионаж и подрывную деятельность, которая включает в себя распространение искаженной информации и дезинформацию. На практике эти действия могут выражаться в отключении или повреждении ключевых объектов инфраструктуры, включая электро- и водоснабжение, больницы, службы наблюдения и пункты связи, а также могут способствовать поражению или выводу из строя военных оборонительных и других систем.

18. В процессе своей работы в интересах частных компаний и государств фирмы, занимающиеся вопросами кибербезопасности, обеспечивают защиту от кибератак и кибервойн. К таким чисто оборонительным операциям относятся брандмауэры, заплатки и антивирусное программное обеспечение, а к более активным, но все же оборонительным шагам — создание приманок и так называемых смоляных ям для программного обеспечения, а также маяков для отпугивания и заманивания в ловушку злоумышленников⁸. Такие оборонительные операции — как пассивные, так и активные — подпадают под существующие правовые нормы для операций по кибербезопасности.

19. Однако как частные, так и государственные фирмы, занимающиеся вопросами кибербезопасности, а также мошенники обладают еще и наступательным потенциалом, что вызывает особую озабоченность у Рабочей группы. Наступательный потенциал фирм, работающих в сфере кибербезопасности, может быть использован против развитых государств, например для атаки на избирательную

⁷ См. документ, представленный организацией ICT for Peace.

⁸ Документ, полученный в запечатанном виде.

инфраструктуру, — для атаки, проводимой, как предполагается, либо государственными учреждениями, либо структурами, работающими на государство. Вредоносная кибердеятельность включает также нападения на виртуальные активы и на поставщиков виртуальных активов, а также на оборонные компании, в том числе с целью получения незаконного доступа к военным технологиям (см. S/2021/211, приложение, пункты 125–126). Нет никакой очевидной и явной объединяющей модели, характеризующей государственных и негосударственных субъектов, приобретающих эти технологии. Как демократические, так и недемократические государства приобретают наступательные технологии у внешних поставщиков — как государства, обладающие собственным киберпотенциалом, так и государства, не имеющие таких ресурсов.

20. Рынок наступательных кибертехнологий быстро растет, слабо регулируется и дает возможность получить значительную прибыль. В результате многие обычные частные военные и охранные компании создают подразделения по кибербезопасности⁹. Независимо от своего происхождения, поставщики услуг кибербезопасности, как и более традиционные частные военные и охранные компании, работают рука об руку с правительствами государств, становятся неким продолжением государственной власти и поэтому могут считаться структурами, действующими как наемники по поручению других лиц.

21. Различия между наступательными и оборонительными услугами и между прозрачностью и двусмысленностью правового статуса затрагивают военные услуги и услуги по обеспечению безопасности, предоставляемые в киберпространстве. Частные структуры могут привлекаться государствами и негосударственными субъектами не только для защиты собственных сетей и объектов инфраструктуры, но и для проведения киберопераций, направленных на ослабление военного потенциала и возможностей вооруженных сил противника или на подрыв целостности территории другого государства. Присутствие наемников в киберпространстве, где они теперь участвуют в производстве и продаже наступательного кибероружия, свидетельствует об их способности приспосабливаться к новым условиям¹⁰. Лица, совершающие кибератаки, могут рассматриваться как осуществляющие деятельность, связанную с наемничеством, или даже занимающиеся наемничеством, если соблюдены все установленные для этого критерии (см. A/75/259, пункт 71).

A. Категории соответствующих киберсубъектов

Киберподразделения или киберкомандования, интегрированные в официальные вооруженные силы

22. В последние годы конкуренция за киберзнания стимулировалась стратегиями кибервливания, которые продемонстрировали свое колоссальное воздействие на современные геополитические отношения¹¹. Некоторые государства участвуют в том, что характеризуется как «информационная борьба в киберпространстве», и включают операции по осуществлению военных стратегий

⁹ W.J. Hennigan, “Defense contractors see opportunity in cybersecurity sector”, *Los Angeles Times*, 21 January. URL: www.latimes.com/business/la-fi-0122-cyber-defense-20150122-story.html.

¹⁰ Tom Burt, “Cyber mercenaries don’t deserve immunity”, Microsoft website, 21 December 2020. URL: <https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/>.

¹¹ См. URL: <https://spire.sciencespo.fr/hdl/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf>, pp. 9–10.

влияния в свой военный потенциал¹². Быстрое развитие цифровых технологий сильно изменило характер войны и побудило делать инвестиции в создание киберподразделений или киберкомандований, интегрированных в официальные вооруженные силы. Кроме того, классические формы войны между противоборствующими вооруженными силами теперь сопровождаются кибервойной, в ходе которой киберподразделения действуют вдоль тонких линий, разделяющих оборонительные и наступательные операции¹³. Кибероперации могут проводиться самостоятельно или в сочетании с традиционными военными операциями. Однако наибольшую тревогу по-прежнему вызывает сценарий «гибридной операции», когда государство отвечает своей кибервоенной операцией на таком фоне, который не считается достигшим порога вооруженного конфликта в соответствии с нормами международного гуманитарного права. Информационная борьба в киберпространстве становится еще более сложной, когда официальные вооруженные силы передают часть своей кибердеятельности третьей стороне.

Действующие лица вне официальных вооруженных сил

23. Негосударственные структуры, не включенные в вооруженные силы, играют весьма существенную и растущую роль в предоставлении киберуслуг государствам и от их имени. Возрастающая угроза приватизации кибератак, совершаемых с помощью нового поколения частных компаний, называемых «кибернаемниками», становится все более распространенной¹⁴, и все более размытой становится грань, разделяющая частную и государственную сферы¹⁵.

Коммерческие предприятия

24. В отличие от обычных частных военных и охранных компаний, которые, как правило, приватизировали функции и возможности, когда-то монополизированные государством, поставщики услуг в области кибербезопасности впервые появились и добились успеха именно в частном секторе. Самые передовые в мире вооруженные силы подготовили собственных специалистов и создали собственные структуры в области кибербезопасности, но даже эти сложные военные операции в значительной степени опираются на знания и опыт частного сектора в сфере кибербезопасности¹⁶. Среди частных компаний, занимающихся вопросами кибербезопасности, есть как давно зарекомендовавшие себя коммерческие игроки, так и умелые начинающие компании, завоевавшие свое место на быстро растущем рынке.

25. Частные компании, занимающиеся разработкой программного обеспечения и технологий, которые попадают в сферу нашего анализа, можно разделить на две группы. Одна подкатегория состоит из крупных технологических платформ, которые работают по согласованию с государственными структурами, чтобы позволить правительству получить доступ к информации и осуществлять программы наблюдения¹⁷. Другая подкатегория состоит из компаний, которые гораздо меньше по своему размеру и по уровню доходов, но имеют конкретные возможности производства продукции, подходящей для ведения вредоносной

¹² См. URL: <https://spire.sciencespo.fr/hdl:/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf>, pp. 7–8.

¹³ Neri Zilber, “The rise of the cyber-mercenaries: what happens when private firms have cyberweapons as powerful as those owned by governments?”, *Foreign Policy* (FP), 31 August 2018. URL: <https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/>.

¹⁴ См. документ, представленный организацией Access Now, стр. 1.

¹⁵ См. документ, представленный Ори Сведом и Даниэлем Бурландом, стр. 15.

¹⁶ См. URL: www.cmi.no/publications/file/6637-russian-use-of-private-military-and-security.pdf.

¹⁷ См. URL: <https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/>.

деятельности. Эта сфера деятельности частных компаний по обеспечению кибербезопасности быстро растет и развивается. Кроме того, несколько частных военных и охранных компаний занялись кибербезопасностью, нередко приобретая мелкие технологические фирмы, чтобы сделать их частью своей компании.

26. Компании оборонного сектора, ранее производившие оружие и военную технику, распространили свою деятельность на цифровой сектор. Эти подрядчики в основном разработали собственные решения и услуги в области кибербезопасности, хотя некоторые из них также наняли коммерческие фирмы по обеспечению кибербезопасности в качестве дочерних компаний для наращивания своих возможностей. В публичной пропаганде оборонных предприятий-подрядчиков умышленно стираются грани между действиями и услугами, предназначенными исключительно для защиты киберпространства, и принципиально новыми технологиями, которые позволят клиентам проводить наступательные операции и потенциально вредоносную деятельность.

Группы, постоянно создающие серьезные угрозы

27. Члены групп, постоянно создающих серьезные угрозы, — это мошенники/преступники, постоянно занимающиеся проникновением в системы кибербезопасности государств, а также государственных и частных структур. Они далеко продвинулись в техническом отношении, обладают значительными финансовыми и техническими ресурсами, имеют долгосрочные стратегические цели и часто пользуются определенной поддержкой со стороны правительств государств¹⁸. Они обладают собственным наступательным потенциалом и могут проводить крупномасштабные кибероперации. Киберподразделения национальных вооруженных сил также постоянно создают серьезные угрозы. «Хакеры, работающие по найму», тоже могут настойчиво проверять надежность киберзащиты частных компаний и правительств. В силу самой своей природы группы, постоянно создающие серьезные угрозы, ассоциируются с более долгосрочными целями, чем получение быстрой прибыли путем вымогательства.

Киберополчение

28. Другая категория включает в себя так называемые киберополчения, которые охватывают различные добровольческие организации. Сами по себе эти ополчения могут быть вне организаций наемников или организаций, связанных с наемниками. Они отличаются от групп, постоянно создающих серьезные угрозы, тем, что не так хорошо организованы, не так хорошо финансируются и не имеют долгосрочных стратегических целей. Теоретическая модель наступательных добровольческих киберополчений проводит различие между форумом, ячейкой и иерархической структурой. Форум представляет собой специальную киберополченческую структуру, организованную вокруг центральной коммуникационной платформы, где участники обмениваются информацией и инструментами, необходимыми для совершения кибератак на выбранную ими цель. Модель ячейки нашла свое воплощение в хакерских ячейках, которые занимаются политически мотивированным взломом в течение длительного времени. Иерархия отражает традиционную иерархическую модель, которая может быть воплощена в виде спонсируемых правительством волонтерских организаций, а также сплоченных негосударственных структур, основанных на принципах самоорганизации. В категорию киберополчений также входят организованные группы

¹⁸ См. URL: <https://targetedthreats.net/media/1-ExecutiveSummary.pdf>.

киберпрофессионалов, которые добровольно участвуют в отражении кибератак¹⁹.

Частные лица

29. Киберэксперты, обладающие техническими знаниями в области информационных технологий, зачастую работают вне всякой организационной структуры и проводят независимые исследования, направленные на обнаружение уязвимостей или ошибок в программном обеспечении²⁰. Этих людей называют исследователями вопросов безопасности, и они могут продавать информацию об этих уязвимостях противникам²¹. В зависимости от конкретных обстоятельств они часто получают плату за эту работу в виде «награды за выявленную ошибку». Они поддерживают связь с потенциальными клиентами через онлайн-порталы.

Киберпреступники

30. Преступные группировки вымогателей — это уголовники, целью которых чаще является не подрыв экономики или политический саботаж, а использование корпоративных данных в качестве механизма вымогательства. Это частные лица или группы, действующие в собственных интересах и направляющие свои усилия на услуги, продукты и объекты инфраструктуры, которые предоставляются государственным и частным секторами и от которых зависят целые сообщества и группы населения. Они требуют выкупа, а реакция на требование этого выкупа со стороны жертв имеет экономические и политические последствия, выходящие за рамки одного конкретного инцидента, поскольку возникает возможность расширения и повторения таких атак. Например, нарушения работы продолжаются до тех пор, пока не будет выплачен какой-то выкуп.

В. Отношения между государственными и негосударственными субъектами

31. Взаимодействие государства с этими субъектами может принимать различные формы. В случае делегирования полномочий государство осуществляет прямой надзор за действиями доверенных лиц посредством проверки и отбора субъектов, применения наказаний и четкой оценки возможных последствий²². В этом случае на доверенных лиц возлагаются ясные обязанности с помощью муниципального законодательства и политики, предусматривающей, например, нанесение упреждающих ударов по предполагаемым источникам киберугроз²³ для важнейших объектов инфраструктуры²⁴. Если же речь идет о манипули-

¹⁹ См. Rain Ottis, “Proactive defense tactics against on-line cyber militia”, in *Proceedings of the 9th European Conference on Information Warfare and Security, Thessaloniki, Greece*, 01–02 July (Reading, United Kingdom, Academic Publishing, 2010), pp. 233–237.

²⁰ Steve Ranger, “Meet the hackers who earn millions for saving the web, one bug at a time”, ZD Net, 16 November 2020. URL: <https://www.zdnet.com/article/meet-the-hackers-who-earn-millions-for-saving-the-web-how-bug-bounties-are-changing-cybersecu/>.

²¹ См. документ, представленный Международной женской лигой за мир и свободу.

²² Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018), p. 29.

²³ Amanda N. Craig, Scott J. Shackelford and Janine S. Hiller, “Proactive cybersecurity: a comparative industry and regulatory analysis”, *American Business Law Journal*, vol. 52, no. 4 (winter 2015).

²⁴ Ellyne Phneah, “Spore beefs up cybersecurity law to allow preemptive measures”, ZDNet, 14 января 2013 г.), Available at www.zdnet.com/sg/spore-beefs-up-cybersecurity-law-to-allow-preemptive-measures-7000009757/.

ровании, то государство оказывает пассивную поддержку своим доверенным лицам, но не создает механизмов прямого надзора за их деятельностью²⁵. Обычно это достигается благодаря слабо определенным или вообще отсутствующим политическим рамкам и благодаря единовременному сотрудничеству путем установления «сетевых отношений»²⁶. Если применяется санкционирующая модель, государство не признает действия частных субъектов, действующих с его территории²⁷.

32. В процессе приватизации некоторых информационных операций и военных стратегий по оказанию влияния государство поручает частным субъектам те задачи, которые оно больше не может или не желает выполнять. Целый ряд поставщиков услуг решает задачи, которые ранее могли выполняться государственными силами безопасности, а также дополнительные задачи, ранее никогда не относившиеся к сфере ответственности государственных сил безопасности (см. A/74/244).

33. Государства поручают оказание киберуслуг негосударственным субъектам по ряду причин. У государств зачастую нет достаточных возможностей для ведения войны традиционными методами, и точно так же некоторые государства могут не обладать достаточным киберпотенциалом, особенно когда соответствующие технологии постоянно развиваются и требуют значительных затрат. Кроме того, государства могут быть не в состоянии поддерживать такой кибернетический потенциал и поэтому могут предпочесть передавать его на внешний подряд на разовой основе. Спрос на киберпотенциал стремительно растет²⁸. Он совпал с острой нехваткой мощностей и возможностей в государствах и был вызван именно этой нехваткой²⁹. Обращение к частным структурам или внешнему подряду может быть обусловлено в некоторых государствах сокращением военного бюджета и более общей тенденцией к привлечению частного сектора к оказанию государству услуг, которые будут включать военные операции и услуги в сфере безопасности³⁰. Кроме того, такой внешний подряд может позволить государствам дистанцироваться от кибердеятельности и избежать пристального внимания и последствий³¹.

34. Рабочая группа отмечает, что сложно выявить с какой-либо степенью уверенности конкретные примеры того, что государства используют наемников и связанных с наемниками субъектов и поручают оказание киберуслуг негосударственным субъектам. Трудно также точно определить объем и характер этих услуг, учитывая крайнюю деликатность таких операций, а также секретность и непрозрачность, типичные для кибериндустрии. Надо провести дополнительные исследования, для того чтобы определить, какие субъекты предоставляют те или иные виды услуг³². Современные исследования о том, как государственные и негосударственные субъекты заключают контракты на использование киберпотенциала и какого рода услуги они приобретают, являются несовершенными и неполными. Отсутствие полноты картины — результат ряда факторов, в

²⁵ Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018).

²⁶ Arindrajit Basu and Elonnai Hickok, "Conceptualizing," Conceptualizing an international framework for active private cyber defense". URL: https://4bac176f-2e16-421b-823f-0ab6d7712f85.filesusr.com/ugd/066049_e1a28ac2850d49fbb6f52eeb9fc79ae7.pdf.

²⁷ Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018).

²⁸ См. документ, представленный Кригом, стр. 1.

²⁹ Там же.

³⁰ Документ, представленный в запечатанном виде.

³¹ См. документ, представленный Кригом, стр. 1.

³² См. документ, представленный организацией ICT for Peace, стр. 2.

том числе того, что большинство компаний, работающих в этом пространстве, являются частными (не зарегистрированными на бирже)³³.

35. Тем не менее полученная информация убедительно свидетельствует о том, что такие контракты и внешние подряды сохраняются и будут использоваться в будущем. Можно также с уверенностью предположить, что они имеют место потому, что индустрия киберуслуг быстро растет, а также вследствие того факта, что еще до повышения роли кибердеятельности государства передавали традиционные функции по обеспечению безопасности и военные функции негосударственным субъектам. Правительства, как правило, не могут угнаться за темпами, с которыми частный сектор разрабатывает новые технологии³⁴. В условиях быстрого развития технологий и на фоне инвестиций в цифровые технологии и искусственный интеллект Рабочая группа выражает твердую убежденность в том, что киберуслуги и киберпродукция будут и впредь передаваться на внешний подряд негосударственным субъектам.

36. Кибератаки совершаются в несколько этапов, поэтому возложить ответственность на злоумышленников и их клиентов очень трудно. Например, при атаке со стороны бот-сети бот-мастер проникает в большую сеть уязвимых компьютеров и заставляет эту сеть взломанных компьютеров атаковать сеть жертвы. Чтобы проследить эту атаку до ее источника — до бот-мастера, надо охватить несколько стран и несколько правовых систем³⁵. Это вызывает серьезные опасения, поскольку кибероперации могут нанести значительный ущерб правам человека. Возможность того, что киберпосредники могут действовать через границы и таким образом оставаться вне поля зрения механизмов регулирования и подотчетности, является серьезной причиной для озабоченности³⁶.

37. Государства, а также негосударственные субъекты начали использовать частных субъектов для проецирования кибермощи, учитывая относительно низкую стоимость таких операций по сравнению с обычными военными действиями и возможность спрятаться за субъектом, идентифицировать которого очень трудно. Использование посредника возводит стену между преступником и его мишенью, и, кроме того, появляется возможность воспользоваться высокой степенью анонимности, доступной в Интернете, и препятствиями, которые возникают перед теми, кто пытается своевременно установить ответственного за данную кибероперацию³⁷. Преимущество использования таких субъектов заключается в том, что, в отличие от государств, на которые распространяются международные документы по правам человека и гуманитарному праву, они действуют вне сферы применения таких документов, что затрудняет присвоение ответственности, арест и судебное преследование³⁸. Это позволяет государству, в свою очередь, отмежеваться от киберопераций и благодаря этому избежать пристального внимания к себе и присвоения юридической и финансовой ответственности³⁹.

³³ См. документ, представленный организацией The Citizen Lab, стр. 1.

³⁴ См. документ, представленный организацией ICT for Peace, стр. 2.

³⁵ David D. Clark and Susan Landau, "Untangling attribution", *Harvard National Security Journal*, vol. 2, No. 2 (2011).

³⁶ Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018).

³⁷ См. документ, представленный Международной женской лигой за мир и свободу, стр. 4.

³⁸ Ataa Dabour, "The rise of cyber-mercenaries", 2021. URL: www.hscentre.org/technology/the-rise-of-cyber-mercenaries/.

³⁹ См. документ, представленный организацией ICT for Peace, стр. 2.

IV. Регулирование роли и участия наемников, субъектов, связанных с наемниками, и частных военных и охранных компаний в предоставлении киберуслуг

38. Регулирование роли и участия наемников, субъектов, связанных с наемниками, и частных военных и охранных компаний в предоставлении киберуслуг, включая кибератаки и кибервойны, на международном уровне сопряжено со значительным количеством проблем и трудностей, в том числе следующего характера: а) разработка концепции кибердеятельности, включая кибервойны и кибератаки; б) выявление источника кибератак и других видов кибердеятельности; с) приписывание таких атак или действий конкретным физическим или юридическим лицам; d) установление характера отношений между негосударственным субъектом и государством, от имени которого осуществляется такая деятельность, если она вообще осуществляется, и вопрос о том, является ли конкретная кибердеятельность доказательством причастности к текущим военным действиям или прямого или косвенного участия в них. Сейчас проводятся многочисленные дискуссии и обсуждения, посвященные степени нынешнего регулирования кибердеятельности и тому, как она должна регулироваться на международном уровне.

39. Эти проблемы обусловлены непрозрачным характером кибердеятельности, ее источником и субъектами, которые ее осуществляют, а также взаимоотношениями между государствами и негосударственными субъектами. Такое размежевание, которое не так легко достижимо в условиях традиционного кинетического вооруженного конфликта, выгодно как государственным, так и негосударственным субъектам, поскольку оно может оградить и тех и других от материальной ответственности за свои действия; в то же время это значительно усложняет регулирование этой деятельности. Вопрос о присвоении ответственности за кибероперации и вопрос о намеренном отмежевании вооруженных сил государства от операций такого рода, с тем чтобы можно было «правдоподобно отрицать» наличие определенной связи между ними, безусловно, серьезно осложняют процесс регулирования.

40. Нынешняя международная нормативная база в этой области включает в себя Устав Организации Объединенных Наций, международное гуманитарное право, Таллиннское руководство по международному праву, применимому к кибервойне, международное уголовное право, международное право в области прав человека, стандарты права и внутригосударственное законодательство.

A. Устав Организации Объединенных Наций

41. Устав Организации Объединенных Наций — и особенно статья 2 (4), которая запрещает угрозу силой или ее применение против территориальной целостности или политической независимости любого государства, — должен играть определенную роль в регулировании и санкционировании кибердеятельности, включая наемничество. Это основано на том, что кибердеятельность может иметь такие масштабы и последствия, которые представляют собой «применение силы» и, следовательно, она может быть запрещена Уставом Организации Объединенных Наций. Точно так же следует отметить, что такая деятельность может превышать порог, определяемый как «вооруженное нападение», а это уже влечет за собой право государства на самооборону в соответствии со статьей 51 Устава Организации Объединенных Наций. Доходит ли такая кибердеятельность до соответствующего «порога», в том числе соответствует ли она

принципам необходимости и соразмерности⁴⁰, — это устанавливается по фактам и масштабам, но вряд ли могут быть сомнения в том, что, учитывая характер и последствия современной кибердеятельности, она вполне может доходить до таких «порогов» в конкретных обстоятельствах.

42. Однако более сложный вопрос, который необходимо рассмотреть, заключается в том, будут ли кибератаки или другие действия, совершаемые негосударственными субъектами, затрагивать соответствующие положения Устава Организации Объединенных Наций. Ответ будет зависеть от того, можно ли будет приписать действия этих физических или юридических лиц конкретному государству согласно Проекту статей об ответственности государств за международно-противоправные деяния, учитывая, что Устав Организации Объединенных Наций применяется только к ситуациям, возникающим между суверенными государствами.

43. Вопрос о присвоении ответственности может вызывать значительные трудности с точки зрения наличия доказательств, поскольку организации, предоставляющие киберуслуги, нередко действуют на значительном удалении от государства, а источник кибератак, вполне вероятно, будет трудно или вообще невозможно установить, поскольку эти кибератаки иницируются на удалении и могут включать в себя различные действия, совершаемые из разных мест и разными субъектами. И, разумеется, есть случаи умышленного использования механизмов, позволяющих избежать обнаружения и присвоения ответственности за атаки.

В. Международные права человека и гуманитарное право

44. Государства обязаны соблюдать международные нормы в области прав человека — как в мирное время, так и во время вооруженного конфликта — с учетом соответствующих конкретных исключений и отступлений. Государства также обязаны гарантировать соблюдение требований частными субъектами на своей территории с помощью внутригосударственного законодательства и правоприменения. Всеобъемлющая и хорошо разработанная система защиты прав человека на международном уровне, с ее различными договорами, органами мониторинга и механизмами обеспечения соблюдения, является готовым средством регулирования киберпространства.

45. В своем заявлении на заседании Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности Международный комитет Красного Креста подтвердил, что нормы международного гуманитарного права применимы к новым формам вооруженных конфликтов, включая кибервойны⁴¹. Этот вывод опирается на Консультативное заключение Международного суда по делу о законности или применении ядерного оружия, в котором Суд решил, что международное гуманитарное право применимо к нынешним и будущим видам оружия и типам ведения войны⁴². Несмотря на продолжающиеся дебаты по поводу конкретной

⁴⁰ См. URL: <https://international-review.icrc.org/articles/can-jus-ad-bellum-override-jus-bello-reaffirming-separation-two-bodies-law>.

⁴¹ Заявление, сделанное Вероникой Кристори, старшим советником по контролю над вооружениями Международного комитета Красного Креста, на заседании Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, Нью-Йорк, 10 сентября 2019 года.

⁴² *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996*, issued on 8 July 1996; ICRC, position Paper on international humanitarian law and cyber operations during armed conflict, November 2019, p. 4.

интерпретации в отношении применения соответствующих принципов международного гуманитарного права к кибероперациям в контексте вооруженного конфликта, складывается впечатление, что в принципе эти правила применимы. Такой подход подтверждается в Таллинском руководстве в отношении права, применимого к кибервойнам. В этом Руководстве однозначно говорится, что «право вооруженных конфликтов применяется к кибероперациям так же, как и к другим операциям, проводимым в условиях вооруженного конфликта».

46. Однако такой подход тоже не лишен трудностей, особенно с учетом роли негосударственных субъектов, предоставляющих такие киберуслуги. Не существует согласованного на международном уровне определения того, что представляют собой в международном гуманитарном праве кибератаки или военные действия в киберпространстве. Однако само понятие «атака» имеет большое значение, прежде всего в связи с принципом, согласно которому проводится различие между военными и гражданскими целями. Военный или гражданский характер целей может быть предметом толкования, но это толкование не зависит от метода ведения войны, использованного для атаки. Независимо от того, совершается ли атака с помощью кинетических средств ведения войны или с использованием кибертехнологий, необходимо уважать гражданский характер объекта.

47. Еще одним вопросом, вызывающим озабоченность, является статус кибероперации во время вооруженного конфликта, а, если говорить конкретно, определение того, считается ли данная операция непосредственным участием в военных действиях, что имеет значение для соответствия критериям классификации в качестве наемника согласно статье 47 Дополнительного протокола I к Женевским конвенциям 1949 года, или имеет достаточную степень связи с конкретным вооруженным конфликтом. В некоторых случаях кибератаки, направленные на уничтожение государственного потенциала и государственной инфраструктуры, приравниваются к прямому участию негосударственного субъекта в военных действиях в ходе вооруженного конфликта⁴³. Может ли какая-либо конкретная кибердеятельность повлиять на военный потенциал одной из сторон в конфликте и может ли она причинить вред одной из сторон в конфликте, если есть достаточная связь между данным действием и вооруженным конфликтом, — это вопрос о фактах и степени интенсивности действий. Этот вопрос имеет не только юридические аспекты, но и более практическое измерение, поскольку не всегда можно установить факт кибератаки или более изощренной кибердеятельности. Интерпретация всех концепций, вероятно, будет зависеть от практики государства.

48. Если говорить более конкретно о наемниках, то лица, отвечающие определению наемника, не имеют права на статус комбатанта и на присущие ему меры защиты. Еще важнее то, что в настоящее время их могут привлечь к судебной ответственности за сам факт их участия в военных действиях, независимо от того, государства или негосударственные субъекты заключили с ними контракт на участие в военных действиях в киберпространстве. Их также могут привлечь к судебной ответственности за то, что они участвовали в наемнической деятельности, при условии, что соответствующий внутренний режим устанавливает такие правовые положения. Кроме того, согласно общей статье 1 Женевских конвенций 1949 года, государства обязаны обеспечивать соблюдение Конвенции, и это включает обеспечение того, чтобы субъекты, действующие от их имени, в

⁴³ Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities, under International Humanitarian Law* (Geneva, ICRC, May 2009). URL: www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf.

том числе негосударственные субъекты, действующие от имени государств, соблюдали международное гуманитарное право.

49. Поэтому было выражено мнение, что традиционное определение наемника может не подходить для случаев, касающихся изменения характера средств ведения войны и современных конфликтов, для которых типично или по крайней мере свойственно использование кибервойн или других видов кибердеятельности, а это говорит о необходимости переосмысления того, что представляет собой наемник, действующий в киберпространстве⁴⁴.

50. Еще один вопрос, который возникает и который необходимо будет рассмотреть в связи с применением международного гуманитарного права к киберпространству, касается различных правовых режимов, которые применяются к немеждународным и международным вооруженным конфликтам, а также того, нужно ли применять такой же подход к киберуслугам. Возникает также вопрос, можно ли по мере развития кибервойн и киберопераций сохранить традиционное различие между международными и немеждународными конфликтами.

51. Кроме того, существует фундаментальная проблема, связанная с тем, что, хотя международное гуманитарное право обеспечивает хорошо разработанную и всеобъемлющую нормативную базу, которую можно применить к кибердеятельности, оно, разумеется, применяется только во время вооруженного конфликта. Дело в том, что многие виды кибердеятельности, а, возможно, и большинство, имеют место вне вооруженных конфликтов, поэтому к ним нельзя применить регулирующий режим, предусмотренный международным гуманитарным правом.

С. Международное уголовное право

52. Международное уголовное право распространяется на любое физическое лицо, совершившее международное преступление, а юрисдикция Международного уголовного суда распространяется на военные преступления, преступления против человечности, геноцид и агрессивную войну. Таким образом, если киберуслуги, предоставляемые физическими лицами, соответствуют одному или нескольким элементам одного или нескольких преступлений и если соблюдены другие соответствующие критерии, Международный уголовный суд потенциально может обладать юрисдикцией в отношении преступных деяний, совершенных в киберпространстве наемниками и связанными с наемниками субъектами. Международное уголовное право может быть полезным в той мере, в какой доктрина ответственности командования может помочь преодолеть некоторые препятствия, связанные с идентификацией и определением местонахождения человека, реально совершившего преступление. Начальники таких лиц, причастные к совершению преступления, например, отдавшие приказ о совершении губительных кибератак или не предотвратившие такие злонамеренные кибератаки, не должны уйти от ответственности⁴⁵. Недостаточно решить только проблемы, упомянутые выше; согласно международному уголовному праву, необходимо, чтобы преступления были доказаны в процессе международного судопроизводства таким образом, чтобы не оставалось никаких разумных сомнений, — это наивысший стандарт доказывания. Кроме того, учитывая, что кибероперации могут затрагивать несколько государств, могут возникать вопросы,

⁴⁴ См. документ, представленный Ван-дер-Вааг-Каулингом, Ван Никерком и д-ром Рамлуканом, стр. 4.

⁴⁵ См. документ, представленный организацией Access Now, стр. 10.

касающиеся юрисдикции и комплементарности, а это может создать дополнительные проблемы для расследований и судебного преследования.

53. Как Международная конвенция о борьбе с вербовкой, использованием, финансированием и обучением наемников, так и Конвенция Организации африканского единства о ликвидации наемничества в Африке предусматривает уголовную ответственность за наемничество, что создает альтернативную правовую основу для преследования и наказания за деятельность, связанную с наемниками. Государства, ратифицировавшие эти конвенции, должны включить соответствующее положение в свой внутригосударственный правовой режим, что позволит национальным судам преследовать наемников.

D. Стандарты права и текущие инициативы

54. Помимо международно-правовых рамок обязывающего характера, за последнее десятилетие появился ряд инициатив, затрагивающих несколько заинтересованных сторон, а также ряд многосторонних инициатив, предназначенных для различных участников и направленных на стимулирование ответственного поведения при использовании информационно-коммуникационных технологий. К ним относятся нормативные, но не имеющие обязательной силы базовые документы, ориентированные на частных субъектов, такие как Техническое соглашение по кибербезопасности и Хартия доверия, разработанные компанией «Сименс». Независимые группы экспертов, такие как Глобальная комиссия по стабильности в киберпространстве и Независимая группа экспертов, разработавшая Таллиннское руководство, подготовили рекомендации по нормам и применимому международному праву. Другие инициативы, затрагивающие несколько заинтересованных сторон, такие как Парижский призыв к доверию и безопасности в киберпространстве, были предназначены для частного сектора, гражданского общества и правительств.

55. В рамках Совета по правам человека важную роль в разработке содержания международной нормативной базы по регулированию, мониторингу и надзору за деятельностью частных военных и охранных компаний играет Межправительственная рабочая группа открытого состава. С учетом быстро меняющихся условий деятельности и предоставляемых услуг любой механизм регулирования, разработанный в рамках этого процесса, должен употреблять термины «услуги» или «деятельность», а не «частные военные и охранные компании», поскольку именно такие термины лучше всего отражают нарушения прав человека или международного гуманитарного права⁴⁶.

56. Для обсуждения более широких вопросов безопасности в области информационно-коммуникационных технологий Генеральная Ассамблея создала две группы, которые в принципе могут дать соответствующие рекомендации: Рабочую группу открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (см. резолюцию 73/27 Ассамблеи) и Группу правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности (см. резолюцию 73/266 Ассамблеи). Работа обеих групп охватывает шесть основных областей: существующие и потенциальные угрозы; правила, нормы и принципы ответственного поведения государств; международное право; меры по укреплению доверия; наращивание потенциала; регулярный институциональный диалог.

⁴⁶ См. Заявление Елены Апарац, Председателя Рабочей группы по использованию наемников. URL: www.ohchr.org/EN/HRBodies/HRC/IGWG_PMSCs/Pages/Session2.aspx.

57. В марте 2021 года Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности приняла одобренный консенсусом доклад, в котором изложены некоторые не имеющие обязательной силы рекомендации для всех государств-членов. Хотя ни одна из этих рекомендаций не затрагивает вопрос о наемниках или связанных с наемниками субъектах, в докладе содержится несколько ссылок на права человека и признается тот факт, что некоторые негосударственные субъекты продемонстрировали свои возможности в сфере информационно-коммуникационных технологий, которые ранее были только у государств. В докладе отмечено, что продолжающееся увеличение числа инцидентов, связанных со злонамеренным использованием информационно-коммуникационных технологий (ИКТ) государственными и негосударственными субъектами, является тревожной тенденцией (см. A/AC.290/2021/CRP.2, пункт 16). В своей резолюции 75/240 от 31 декабря 2020 года Генеральная Ассамблея постановила создать новую Рабочую группу открытого состава на период до 2025 года, а Рабочая группа по вопросу об использовании наемников как средстве нарушения прав человека и противодействия осуществлению права народов на самоопределение считает, что благодаря этому появится важная возможность обсудить вопрос о наемниках и связанных с наемниками субъектах, действующих в киберпространстве.

58. В своем одобренном консенсусом докладе за 2021 год Группа правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности подтвердила, что «государства не должны использовать посредников для совершения международно-противоправных действий с использованием ИКТ и должны стремиться к тому, чтобы их территория не использовалась негосударственными субъектами для совершения таких действий»⁴⁷. Хотя это не означает установления правового стандарта для государств, это положение отражает стремление осудить государственное манипулирование и санкционирование деятельности пособников. Группа правительственных экспертов отметила, что усилия государств по поощрению уважения и соблюдения прав человека и обеспечению ответственного и безопасного использования информационно-коммуникационных технологий (ИКТ) должны быть взаимодополняющими, взаимоусиливающими и взаимозависимыми, признавая при этом, что массовое отслеживание может иметь негативные последствия для прав человека, включая право на частную жизнь⁴⁸.

59. Новые инициативы по установлению стандартов были представлены как «комплекс режимов» по обеспечению кибербезопасности, включающий в себя не один главный юридически обязывающий документ, а целый комплекс усилий.

V. Последствия для прав человека

60. Бесспорно, что кибердеятельность затрагивает нормы и стандарты прав человека и способна привести к нарушениям — как в условиях вооруженных конфликтов, так и в мирное время — а, значит, затрагивает целый ряд прав. Рабочая группа пришла к выводу, что связанные с гендерными аспектами риски и последствия деятельности частных военных и охранных компаний, независимо от их размера и объема предоставляемых услуг, имеют много общих черт (см. A/74/244, пункт 6). Кроме того, Рабочая группа выявила слои населения, которые особенно страдают от наемников и связанных с наемниками субъектов, нанятых государствами, такие как правозащитники, мигранты, лидеры

⁴⁷ См. URL: <https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf>, para. 71 g).

⁴⁸ Ibid., paras. 39 and 37.

оппозиции и журналисты, а также лесбиянки, гомосексуалы, бисексуалы, транс-гендеры, интерсексуалы и лица нетрадиционной гендерной ориентации в контексте гендерного насилия.

61. Новые и только появляющиеся формы ведения войны могут оказывать значительное воздействие как на военные цели, так и на гражданское население и могут приводить к нарушениям международного гуманитарного права, а также прав и свобод человека в условиях вооруженных конфликтов и в иных ситуациях. Рабочая группа ранее указывала, что кибервойна признана методом ведения войны, с помощью которого можно не только проникать на военные или гражданские объекты, нарушать их функционирование, наносить им ущерб и даже уничтожать их, но и причинять серьезный вред людям⁴⁹. Киберсаботаж может иметь огромные вторичные последствия для работы важнейших объектов инфраструктуры, потенциально подрывая здоровье и безопасность населения. В этом контексте право на жизнь и право не подвергаться пыткам и другим бесчеловечным или унижающим достоинство видам обращения являются основными правами, которые могут быть нарушены в результате киберопераций.

Право на неприкосновенность частной жизни и свободу выражения мнений

62. Во всех ситуациях право на неприкосновенность частной жизни и право на свободу выражения мнений находятся под угрозой нарушения. Когда наемники и связанные с наемниками субъекты готовятся к нападению на государства, они неизбежно становятся ключевыми инструментами подрыва суверенитета и территориальной целостности таких государств, что также препятствует осуществлению права на неприкосновенность частной жизни.

63. Право на неприкосновенность частной жизни также может быть нарушено в результате мониторинга и сбора оперативной информации. Назрела серьезная озабоченность по поводу киберопераций, направленных против гражданского общества, особенно против правозащитников и журналистов, с целью сорвать их деятельность для подавления инакомыслия и усиления контроля государства над своим населением. Хотя правительства уже давно используют различные методы для наблюдения и слежки за своими гражданами, диссидентами, политическими оппонентами и правозащитниками, доступные сегодня технологические инструменты, такие как вредоносные и шпионские программы, позволяют им делать это с меньшими затратами, расширять географию наблюдения и увеличивать его масштабы, тем самым позволяя правительствам осуществлять цифровые репрессии более масштабно, чем когда-либо прежде⁵⁰. Некоторые формы шпионских программ являются хрестоматийными примерами инструментов, позволяющих удаленно следить за объектами⁵¹.

64. Кроме того, было высказано предположение, что право на свободу выражения мнения может быть нарушено в результате контроля, осуществляемого некоторыми государствами над интернет-контентом или распространением дезинформации и искаженной информации. Подрывные кибероперации, проводимые государственными заказчиками или по их поручению, могут подорвать целостность киберпространства, свободу слова и другие гражданские свободы не только отдельных лиц, но и групп и общества в целом⁵². Целенаправленная слежка также создает стимулы для самоцензуры и напрямую подрывает

⁴⁹ МККК, «Международное гуманитарное право и кибероперации во время вооруженных конфликтов», документ с изложением позиции, ноябрь 2019 года.

⁵⁰ См. документ, представленный организацией The Citizen Lab, стр. 8.

⁵¹ A/HRC/41/35, пункт 9; Bill Marczak and others, *Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries*, Citizen Lab, 18 September 2018.

⁵² S/2021/569, пункт 103.

способность журналистов и правозащитников проводить расследования и выстраивать и поддерживать отношения с источниками информации⁵³.

65. Технологии наблюдения, разработанные, поддерживаемые и иногда эксплуатируемые частными компаниями, также играют важную роль в смещении маршрутов миграции в сторону от подконтрольных районов в районы, находящиеся вне зоны наблюдения. Поэтому мигранты вынуждены выбирать менее прямые и более опасные маршруты в ходе миграции по воде или суше, что увеличивает физические трудности передвижения и связанные с этим физиологические и психические нагрузки, боль и страдания, которые зачастую приводят к гибели из-за теплового удара, сильного обезвоживания и других перипетий⁵⁴.

66. Возможности кибертехники оказывают существенное пагубное влияние как на учреждения, так и на людей, подрывая способность правительств обеспечивать защиту и благополучие значительной части населения и препятствуя осуществлению прав человека. Например, атаки на избирательные системы напрямую влияют на осуществление основных демократических прав, касающихся представительства граждан, поскольку их лишают права голоса. Также сообщалось, что некоторые страны регулярно совершают кибератаки на гражданские сферы, взламывают частные компании или подрывают иностранные вооруженные силы, используя онлайн-инструменты для манипулирования информацией, цифровую пропаганду для формирования мнения других людей и кибернаемников для выполнения этой работы⁵⁵.

67. Поступают сообщения о кибератаках, наносящих большой физический ущерб, в том числе электросетям, финансовым учреждениям и правительственным министерствам⁵⁶. Уничтожение баз данных, содержащих информацию о гражданских лицах, может быстро привести к полной остановке работы государственных служб и частного бизнеса и тем самым причинить больше вреда гражданским лицам, чем уничтожение физических объектов⁵⁷.

Самоопределение

68. Что касается права на самоопределение, то благодаря использованию в киберпространстве продуктов и услуг, предназначенных для военных целей и обеспечения безопасности, фирмы, занимающиеся вопросами кибербезопасности, могут активно препятствовать осуществлению права народов на самоопределение. Эти субъекты способны влиять на внутригосударственные повстанческие движения таким образом, что в итоге могут подорвать право на самоопределение (см. A/71/318, пункт 20).

⁵³ См. A/HRC/38/35/Add.2, пункт 53; A/HRC/41/35, пункт 26.

⁵⁴ A/HRC/45/9, пункты 44–45.

⁵⁵ Paul D. Shinkman, "America Is losing the cyber war", U.S. News and World Report website, 29 September 2016. URL: www.usnews.com/news/articles/2016-09-29/cyber-wars-how-the-us-stacks-up-against-its-digital-adversaries.

⁵⁶ Neri Zilber, "The rise of the cyber-mercenaries: what happens when private firms have cyberweapons as powerful as those owned by governments?", *Foreign Policy* (FP), 31 August 2018. URL: <https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/>.

⁵⁷ МККК, «Международное гуманитарное право и кибероперации во время вооруженных конфликтов», документ с изложением позиции, ноябрь 2019 года.

VI. Выводы и рекомендации

69. Развитие и цифровизация технологий оказывают непосредственное влияние на все сферы гражданской жизни. Военная сфера также все больше зависит от цифровых технологий. Растущая тенденция к цифровизации выражается в усилении слияния информационного пространства и киберпространства и может оказывать негативное воздействие на население в мирное время и в течение вооруженных конфликтов.

70. Рабочая группа приняла во внимание эволюцию сферы предоставления военных продуктов и услуг по обеспечению безопасности в киберпространстве наемниками, субъектами, связанными с наемниками, и частными военными охранными компаниями и соответствующие последствия для осуществления прав человека. Она отметила проблемы, возникающие вследствие попыток сосредоточиться исключительно на деятельности, отвечающей определению термина «наемник» в соответствии с применимой международно-правовой базой, и использовала более широкий подход, изучив различные субъекты и проявления, которые подходят под более гибкую концепцию деятельности, связанной с наемничеством.

71. Рабочая группа с озабоченностью отметила, что некоторые государства умышленно или неосознанно скрывают свое участие в злонамеренных кибероперациях, стремясь получить стратегическое военное влияние, уходя от ответственности по международному праву, в том числе за нарушения и злоупотребления, совершенные негосударственными субъектами, завербованными с этой целью. Однако привлечение частных субъектов для оказания военных услуг и услуг по обеспечению безопасности в киберпространстве не освобождает государства от их обязательств по международному праву.

72. Поэтому новые и еще только формирующиеся проявления деятельности структур, связанных с наемниками, требуют срочного внимания со стороны государств и других соответствующих заинтересованных сторон. В настоящем докладе изложены соображения, которые надо принять во внимание для поддержки государств и других субъектов при разработке более эффективных методов регулирования деятельности субъектов в киберпространстве с целью обеспечения уважения, защиты и реализации права народов на самоопределение, защиты гражданского населения в ситуациях вооруженного конфликта и соблюдения принципов невмешательства и территориальной целостности. Обсуждения любого регулирования должны опираться на международную правовую базу, касающуюся наемников, несмотря на ее недостатки, а также на более широкие рамки международного гуманитарного права и права, регулирующего права человека.

Рекомендации

73. Для предотвращения и смягчения негативного воздействия на права человека, оказываемого наемниками и связанными с наемниками субъектами, а также частными военными и охранными компаниями в киберпространстве, государства должны воздерживаться от вербовки, использования, финансирования и обучения наемников, запрещать такое поведение во внутригосударственном законодательстве и эффективно регулировать деятельность частных военных и охранных компаний.

74. Государства должны заявить о своей приверженности принципу прозрачности в отношении заключения контрактов на оказание вспомогательных военных услуг, в том числе для киберопераций, должны обеспечить

такую прозрачность на практике и обнародовать достаточно подробную и своевременную информацию о характере услуг, процедурах закупок, условиях контрактов и названиях поставщиков услуг. Они не должны ссылаться на соображения национальной безопасности в качестве типичной причины ограничения доступа к такой информации; вместо этого ограничения доступа к информации должны отвечать критерию законности, необходимости и соразмерности в соответствии с правом на свободу выражения мнения.

75. Государства должны расследовать, преследовать и наказывать за предполагаемые нарушения международного гуманитарного права и прав человека наемниками, субъектами, связанными с наемниками, и частными военными и охранными компаниями, а также предоставлять эффективные средства правовой защиты жертвам. Расследования, судебные преследования и судебные процессы должны проводиться на основе уважения и гарантирования права на справедливое судебное разбирательство и надлежащую правовую процедуру.

76. На международном уровне государства должны начать диалог о новых и эволюционирующих формах наемничества, в том числе о наемниках, действующих так или иначе в киберпространстве, о рисках, которые они создают для международного гуманитарного права и международного права в области прав человека, и о путях их более эффективного преодоления и пресечения. Любой такой диалог должен включать международные и региональные организации, гражданское общество и экспертов и учитывать существующие инструменты и инициативы.

77. Государствам следует активизировать обсуждения с Межправительственной рабочей группой открытого состава по разработке содержания международной нормативной базы регулирования, мониторинга и контроля деятельности частных военных и охранных компаний, в том числе в отношении случаев, когда они предоставляют киберуслуги и действуют в условиях кибервойн⁵⁸. Необходим юридически обязывающий документ, регулирующий киберпространство. Международная правовая база приведет к определенности и предсказуемости благодаря четким правовым обязательствам, выполнение которых можно обеспечить с помощью специальных механизмов урегулирования споров. Фрагментация регламентирующих режимов только вносит путаницу в систему регулирования и часто ставит в невыгодное положение развивающиеся страны и гражданское общество.

78. Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и Группа правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности должны продолжить рассмотрение проблем прав человека, возникающих в связи с участием наемников и связанных с ними субъектов в кибероперациях.

79. Что касается деятельности наемников, деятельности, связанной с наемничеством, и деятельности частных военных компаний и компаний, занимающихся вопросами безопасности, которые связаны с вооруженными негосударственными субъектами, то государствам следует согласовывать и поддерживать международные процессы по выявлению, оценке и дальнейшему развитию механизмов более конкретного и официального признания

⁵⁸ См. резолюцию 36/11 Совета по правам человека.

международных обязательств вооруженных негосударственных субъектов в области прав человека, включая критерии для определения способности вооруженных негосударственных субъектов выполнять обязательства в области прав человека.
