



Генеральная Ассамблея

Distr.: General
23 July 2024
Russian
Original: English

Семьдесят девятая сессия

Пункт 97 предварительной повестки дня*

Роль науки и техники в контексте международной безопасности и разоружения

Последние достижения в области науки и техники и их потенциальное воздействие на усилия в области международной безопасности и разоружения

Доклад Генерального секретаря

Резюме

Во исполнение резолюции [78/22](#) Генеральной Ассамблеи в настоящем докладе представлен обзор научно-технических достижений, имеющих отношение к оружию, средствам или методам ведения войны, и их потенциального воздействия на усилия в области международной безопасности и разоружения, а также событий, происходящих в рамках соответствующих межправительственных форумов. В нем охвачены такие вопросы, как искусственный интеллект и автономность, беспилотные системы, цифровые технологии, разработки в области биологии и химии, космические и аэрокосмические технологии, электромагнитные технологии и технологии материалов. Кроме того, в докладе рассматривается вопрос о конвергенции технологий.

* [A/79/150](#).



I. Введение

1. В пункте 4 своей резолюции [78/22](#) по вопросу о роли науки и техники в контексте международной безопасности и разоружения Генеральная Ассамблея просила Генерального секретаря представить Ассамблее на ее семьдесят девятой сессии обновленный доклад о последних достижениях в области науки и техники и их потенциальном воздействии на усилия в области международной безопасности и разоружения.
2. Наука и техника способствуют развитию человеческого потенциала и процветанию человека и являются ключевыми факторами, подкрепляющими усилия по претворению в жизнь Повестки дня в области устойчивого развития на период до 2030 года. Как отметил Генеральный секретарь в своей концептуальной записке, посвященной «Новой повестке дня для мира» ([A/77/CRP.1/Add.8](#)), важно не допускать того, чтобы шаги, предпринимаемые для устранения опасностей применения новых и новейших технологий в качестве оружия, ограничивали странам глобального Юга доступ к огромным преимуществам, которые сулят такие технологии для достижения целей в области устойчивого развития.
3. Однако продолжает вызывать беспокойство то, что научно-технический прогресс в областях, имеющих отношение к безопасности и разоружению, опережает развитие нормативных правовых и управленческих баз в части управления рисками. Преимущества новых и новейших технологий не должны причинять ущерб глобальной безопасности. Для сведения к минимуму вреда и устранения сквозных рисков, порождаемых стремительными темпами развития технологий и их конвергенцией, необходимо внедрить механизмы регулирования (там же, действие 11).
4. В настоящем докладе представлен обзор научно-технических достижений, имеющих непосредственное отношение к оружию, средствам или методам ведения войны, и их потенциального воздействия на усилия в области международной безопасности и разоружения, а также событий, происходящих в рамках соответствующих межправительственных форумов.

II. Последние достижения в области науки и техники, имеющие отношение к оружию, средствам или методам ведения войны

A. Искусственный интеллект и автономность

5. Системы искусственного интеллекта могут интегрироваться в целый ряд приложений, поддерживающих принятие решений, планирование и логистику в военной сфере и обеспечивающих автономность систем оружия, включая автономные функции для применения смертоносной силы. Слияние искусственного интеллекта с другими областями науки и техники может создавать новые каналы для распространения оружия, а также средств и методов ведения войны. Искусственный интеллект, разработанный для гражданских целей, может использоваться не по назначению, в том числе для политической дезинформации, кибератак, террористических актов или других злонамеренных действий, что создает значительные риски для технологий двойного назначения и международного управления.
6. Помимо стремительных достижений в области гражданского искусственного интеллекта, все чаще поступают сообщения о применении государствами систем с искусственным интеллектом в военном контексте, и растет

озабоченность по поводу приобретения таких технологий негосударственными субъектами. Хотя в настоящее время исследования и разработки в области искусственного интеллекта сосредоточены в небольшом числе государств и осуществляются в основном частными компаниями, неосязаемый и быстро меняющийся характер технологий создает трудности в плане мониторинга и регулирования таких технологий и управления ими.

7. Особую озабоченность вызывает вопрос о том, как проводить обстоятельные испытания, обеспечивающие надежность, безопасность, защищенность и точность систем искусственного интеллекта в военной сфере. Несмотря на всеобщее признание того, что искусственный интеллект в военной сфере должен быть «устойчивым» (т. е. технически надежным и безопасным), вероятные различия между условиями испытаний и развертывания ставят вопросы о том, как обеспечить такую устойчивость, в том числе в отношении потенциальных нарушений международного гуманитарного права. Так, при использовании в таких целях, как выбор цели в автономных системах оружия и системах поддержки принятия решений, приложения искусственного интеллекта могут бросать вызов принципу избирательности, в частности из-за проблем с надежностью данных, ошибок в распознавании образов и отсутствия понимания контекста. Если такие приложения используются для нанесения ударов в больших или неизбежных масштабах, они могут противоречить принципам соразмерности и предосторожности.

8. Стремительное развитие генеративного искусственного интеллекта является важным событием и особо указывает на масштабы данных и вычислительных ресурсов, которые определяют современный искусственный интеллект. Большие языковые модели представляют собой разновидность фундаментальных моделей и обучаются на основе обширных данных, которые могут адаптироваться к ряду последующих задач, включая потенциальное применение в военных целях. Стремительное расширение использования больших языковых моделей и выпуск моделей с открытым исходным кодом, обеспечивающих более широкий доступ, создают потенциальные риски для международного мира и безопасности — начиная от умышленного использования не по назначению для создания новых видов оружия, средств и методов ведения войны и заканчивая множеством рисков, связанных с применением в военных целях, которые могут возникать даже при использовании технологий ответственными субъектами¹. Компромиссы в части обеспечения прозрачности искусственного интеллекта являются важной темой текущей дискуссии о необходимости сохранения традиции открытости, которая может способствовать инновациям и развитию, и необходимости надзора.

Соответствующие межправительственные процессы, органы и документы

9. На состоявшемся в 2023 году совещании Высоких Договаривающихся Сторон Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие, было решено продолжить работу Группы правительственных экспертов по новейшим технологиям в сфере смертоносных автономных систем вооружений. Было также решено, что Группа должна продолжать рассмотрение и сформулировать на основе консенсуса набор элементов документа, не предпреляя его характер, и другие возможные меры по решению проблемы новейших технологий в области смертоносных автономных систем вооружений, принимая во внимание пример существующих

¹ Степень преимущества моделей с открытым исходным кодом для потенциального вредоносного использования все еще обсуждается.

протоколов в рамках Конвенции, предложения, представленные высокими договаривающимися сторонами, и другие варианты, связанные с нормативной и оперативной базой по новейшим технологиям в области смертоносных автономных систем вооружений, опираясь на рекомендации и выводы Группы и привлекая экспертов по правовым, военным и технологическим аспектам. Группа высказала мнение, что в системах вооружений, основанных на новейших технологиях в области смертоносных автономных систем вооружений, используются наборы данных, которые могут увековечивать или усиливать неумышленно сформировавшиеся социальные стереотипы, включая гендерные и расовые предубеждения, и тем самым могут иметь последствия для соблюдения норм международного права.

10. Несмотря на наличие сторонних инициатив, в настоящее время под эгидой Организации Объединенных Наций не осуществляется никаких межправительственных процессов по проблеме ответственного жизненного цикла искусственного интеллекта в военной сфере.

В. Беспилотные системы

11. Беспилотные системы могут управляться в дистанционном, полуавтономном или автономном режиме и применяются в воздухе, на суше и на море. Наиболее широко распространены по-прежнему беспилотные авиационные системы, хотя ширятся масштабы разработки и применения морских и наземных систем. Области применения беспилотных систем включают военное наблюдение и разведку, целеуказание и операции по нанесению ударов.

12. Универсальность беспилотных систем и их способность снижать угрозу для жизни оператора по сравнению с угрозой, которой подвергаются экипажи пилотируемых систем, обеспечивают все большую привлекательность беспилотных систем как для государственных, так и негосударственных субъектов. Беспилотные летательные аппараты, в частности, нашли широкое применение в конфликтах, поскольку их производство зачастую обходится дешевле и занимает меньше времени, чем производство сопоставимых пилотируемых систем. Беспилотные системы могут быть как ударными, так и неударными. Одним из примеров являются барражирующие боеприпасы, представляющие собой ударные авиационные системы одноразового применения, которые сочетают в себе характеристики беспилотных авиационных систем и ракет, в результате чего сама система является оружием, барражируя в воздушном пространстве до нанесения удара. Недавнее применение беспилотных систем в населенных районах вызвало обеспокоенность по поводу защиты гражданского населения и соблюдения норм международного гуманитарного права, в том числе из-за возможности нанесения крупномасштабных ударов по целям, находящимся далеко от линии фронта. Кроме того, применение вооруженных беспилотных систем чревато опасностью снижением порога применения силы — отчасти из-за меньшей степени восприятия риска для человека-оператора.

13. Научно-технические разработки направлены на улучшение характеристик отдельных компонентов, входящих в состав беспилотных систем, а также всех систем в целом в целях повышения их живучести, надежности и эксплуатационных характеристик². Однако беспилотные системы уязвимы для помех, в том числе для глушения или подмены данных наблюдения, связи и систем позиционирования. Интеграция искусственного интеллекта — один из методов

² United Nations Institute for Disarmament Research (UNIDIR), “Uncrewed aerial, ground, and maritime systems: a compendium”, April 2023.

повышения автономности и снижения зависимости от потенциально уязвимых каналов связи (см. также разделы II.A и II.F).

Соответствующие межправительственные процессы, органы и документы

14. В своей резолюции [2370 \(2017\)](#) Совет Безопасности решительно осудил непрекращающийся поток оружия, включая беспилотные авиационные системы и их компоненты, которые поступают незаконным вооруженным группам, террористам и другим несанкционированным получателям и циркулируют между ними, и рекомендовал государствам-членам предотвращать и пресекать деятельность сетей по закупке такого оружия, систем и компонентов. В 2022 году была принята Делийская декларация о противодействии применению новых и новейших технологий в террористических целях³. В 2023 году в соответствии с этой декларацией были подготовлены Абу-дабийские руководящие принципы в отношении беспилотных авиационных систем (см. [S/2023/1035](#)).

15. Что касается повышения прозрачности в вооружениях и поощрения их ответственной передачи, то беспилотные системы прямо включены в категорию IV («Боевые самолеты и боевые беспилотные летательные аппараты») и категорию V («Боевые вертолеты и боевые винтокрылые беспилотные летательные аппараты») Регистра обычных вооружений Организации Объединенных Наций. Некоторые государства — участники Договора о торговле оружием включали информацию о беспилотных системах в свои доклады, представляемые в соответствии с Договором.

С. Цифровые технологии

16. Все больше усиливается зависимость от цифровых технологий, которые продолжают развиваться стремительными темпами. И далее неуклонно развивается интернет вещей: по оценкам, к нему подключено 7 миллиардов устройств, и к 2025 году их число возрастет до 22 миллиардов⁴. Прорыв в области цифровых технологий, включая информационно-коммуникационные технологии (ИКТ), квантовые технологии, облачные вычисления, технологии блокчейн, сети 5G и искусственный интеллект, продолжает открывать возможности для преобразования отраслей, экономики и общества.

17. Более широкое использование цифровых технологий открывает перед обществом беспрецедентные возможности. Однако эксплуатация новых уязвимостей и злонамеренное применение таких технологий чреваты последствиями для международного мира и безопасности. Злонамеренная деятельность может иметь каскадные последствия на субрегиональном, региональном и глобальном уровнях. Помимо прямых последствий для населения, вызванных воздействием на критически важную инфраструктуру, злонамеренные действия с применением цифровых технологий могут также подрывать доверие к избирательным процессам и государственным институтам и негативно сказываться на конфиденциальности, целостности и доступности данных.

Информационно-коммуникационные технологии

18. Растет число случаев злонамеренного применения ИКТ как государственными, так и негосударственными субъектами. В 2023 году поступала информация о серьезных инцидентах, в том числе оказывавших воздействие на

³ См. https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/outcome_document_ctc_special_mtg_final_e.pdf.

⁴ См. <https://www.oracle.com/internet-of-things/what-is-iiot/>.

инфраструктуру, используемую для предоставления основных услуг населению в таких областях, как здравоохранение, банковские операции и гражданские телекоммуникации. Также продолжалась эксплуатация уязвимостей программного обеспечения, в том числе путем коммерческой продажи информации о таких уязвимостях через интернет.

19. В прошедшем году некоторые государства сообщали о значительном увеличении числа инцидентов, связанных с программами-вымогателями, отмечая при этом рост преступной, финансово мотивированной деятельности⁵. По некоторым оценкам, в 2023 году объем выплат вымогателям достиг в общей сложности 1,1 млрд долл. США⁶. Кроме того, в различных регионах продолжало документально фиксироваться распространение — с разной степенью воздействия — различных видов вредоносного программного обеспечения, таких как «зловредны», «вайперы» и «трояны», в сочетании с более широким применением таких приемов, как фишинг, вредоносная эксплуатация облачных сред и распределенные атаки на отказ в обслуживании. Все большую обеспокоенность вызывает распространение имеющихся в продаже средств кибервмешательства, включая шпионские программы и другие «наборы для вредоносной эксплуатации»⁷. Сообщалось также, что вредоносная деятельность, направленная на производственно-сбытовые цепочки таких компаний, как поставщики программного обеспечения, имела разрушительные последствия⁸.

20. Диверсификация субъектов и методов продолжала осложнять картину угроз. Негосударственные субъекты, включая преступные организации, террористов, хакерские группы и отдельных лиц, применяли различные инструменты, приемы, средства эксплуатации уязвимостей и векторы атак в целях нарушения работы сетей, приложений и контента и их уничтожения.

Квантовые технологии

21. Государства все чаще обращают внимание на потенциальные последствия применения новых квантовых технологий для международного мира и безопасности. Интеграция квантовых свойств в такие функции, как вычисление, коммуникация, распознавание, визуализация и криптография, способна оказывать значительное благотворное трансформирующее воздействие, в том числе на международный мир и безопасность. Так, например, квантовые компьютеры позволяют многократно увеличить скорость вычислений и будут способны решать более сложные задачи. Квантовое распознавание и квантовая визуализация позволяют фиксировать объекты с такой четкостью, которую не могут обеспечить классические сенсорные технологии, а постквантовая криптография считается весьма безопасной.

22. Однако помимо таких потенциальных преимуществ, квантовые технологии несут в себе и потенциальные риски для международного мира и безопасности. Так, квантовые вычисления предположительно создадут проблемы для ныне существующих криптографических систем, сделав цифровую инфраструктуру, включая инфраструктуру, используемую для предоставления основных услуг

⁵ См. <https://www.cisa.gov/stopransomware/official-alerts-statements-cisa>.

⁶ Alexander Culafi, “Chainalysis: 2023 a ‘watershed’ year for ransomware”, TechTarget, 7 February 2024.

⁷ См. <https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities>.

⁸ Karamveer Singh Sidhu, “Top 5 famous software supply chain attacks in 2023”, CloudSEK, 24 November 2023.

населению, уязвимой для целенаправленной вредоносной деятельности. Также следует отметить потенциальное увеличение числа атак по принципу «собери сейчас, расшифруй позднее», когда злоумышленники накапливают конфиденциальные зашифрованные данные, понимая, что технология позволит расшифровать их впоследствии.

23. Несмотря на то, что влияние квантовых технологий будет предположительно далеко идущим, в настоящее время в национальные программы соответствующих исследований и разработок вкладывают средства менее 20 стран. Во избежание углубления технологического разрыва важно обеспечить инклюзивность образования в части квантовых технологий.

Сети 5G

24. Благодаря повсеместному распространению технологий сотовой связи пятого поколения, известных как 5G, совершается революция в сфере коммуникаций, позволяющая значительно увеличить скорость загрузки и выгрузки данных, а также сократить время, необходимое для обмена данными между подключенными устройствами. В процессе перехода на технологию 5G появляются новые возможности и уязвимости. Эта технология получила множество положительных отзывов как позволяющая, в частности, улучшить связуемость для «умных» городов, телемедицины и обеспечения общего экономического роста. Однако при этом были выявлены и риски, такие как злонамеренное или неумышленное внедрение уязвимостей на этапе проектирования. Существует также возможность появления или возникновения уязвимостей в производственно-сбытовых цепочках и связанной с ними архитектуре 5G.

Соответствующие межправительственные процессы, органы и документы

25. Вопрос о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности стоит на повестке дня Генеральной Ассамблеи с 1998 года⁹. В результате обсуждений в группах экспертов и рабочих группах открытого состава были выработаны рекомендации по нормам, правилам и принципам ответственного поведения государств, мерам укрепления доверия и наращивания потенциала, при этом рассматривается вопрос о том, как применяется к использованию таких технологий международное право (см. A/65/201, A/68/98, A/70/174 и A/76/135). Параллельно с работой шестой Группы правительственных экспертов по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности Генеральная Ассамблея своей резолюцией 73/27 учредила рабочую группу открытого состава по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности. В марте 2021 года Группа утвердила консенсусом доклад (A/75/816), который был одобрен Генеральной Ассамблеей в ее решении 75/564.

⁹ Более подробную информацию о межправительственных обсуждениях вопроса о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности см. на сайте www.un.org/disarmament/ict-security.

26. В 2020 году Генеральная Ассамблея учредила еще одну рабочую группу открытого состава по безопасности информационно-коммуникационных технологий и их безопасному использованию с пятилетним мандатом, в частности, для целей дальнейшей разработки правил, норм и принципов ответственного поведения государств; дальнейшего изучения существующих и потенциальных угроз в сфере информационной безопасности и вопроса о том, как применяется к использованию информационно-коммуникационных государствами международное право; и рассмотрения мер по укреплению доверия и наращиванию потенциала. Соответственно в июле 2022 года и в 2023 году рабочая группа утвердила свой первый и второй доклады о проделанной работе ([A/77/275](#) и [A/78/265](#)), в которых содержатся рекомендации в отношении ряда последующих шагов, включая создание глобального межправительственного реестра контактных пунктов. В этих докладах было признано наличие «гендерного цифрового разрыва» и была подтверждена необходимость усилий по наращиванию потенциала с учетом гендерного фактора.

27. Под эгидой рабочей группы открытого состава государства продолжали рассматривать существующие и возникающие угрозы безопасности в сфере ИКТ. Государства по-разному оценивают воздействие на международный мир и безопасность цифровых технологий, включая ИКТ, искусственный интеллект и квантовые технологии, в том числе последствия их конвергенции.

D. Биология и химия

28. Норма, запрещающая враждебное использование химии и биологии, существует на протяжении длительного времени и закреплена в международном праве благодаря Конвенции 1972 года о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении и Конвенции 1993 года о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении. Однако наблюдающиеся в последнее время случаи применения химических веществ в качестве оружия, заявления о разработке биологического оружия и достижения в области химии и биологии угрожают подорвать эти нормативно-правовые меры.

29. Достижения в области биологии и химии ускоряются и становятся все более взаимосвязанными. В целом, такие достижения открывают ряд возможностей для решения социальных проблем. Однако они могут создавать и риски для международного мира и безопасности.

30. Одобрение применения терапии редактирования генов с использованием кластерных регулярно чередующихся коротких палиндромных повторов (CRISPR) для лечения серповидно-клеточной болезни и трансфузионно-зависимой бета-талассемии продемонстрировало потенциал такой технологии в лечении ранее не поддававшихся лечению заболеваний¹⁰. Однако возможность редактировать гены заключает в себе и значительные риски. Теоретически, те же методы могут использоваться для усовершенствования агентов, использовавшихся в предыдущих программах по биологическому оружию, или для создания новых форм биологического оружия. Во избежание такого злонамеренного применения технологий требуется обеспечить надежное регулирование, международное сотрудничество и целенаправленное изучение непредвиденных

¹⁰ Cormac Sheridan, “The world’s first CRISPR therapy is approved: who will receive it?”, *Nature Biotechnology*, том 42, No. 1 (January 2024); Willow Shah-Neville, “A gene editing milestone: the FDA approves CASGEVY, the first CRISPR-based therapy”, Labiotech, 11 December 2023.

последствий редактирования генов, с тем чтобы эти инновации приносили пользу человечеству, а не создавали неоправданных рисков для него.

31. Начало испытаний технологии нейроинтерфейса на людях приблизило сопряжение когнитивных способностей человека и машин. В 2024 году была проведена первая имплантация нейроинтерфейса человеку частной компанией. Открываются захватывающие перспективы для медицины: можно восстанавливать утраченные сенсорные функции или способствовать лечению нарушений мозговой деятельности. Однако последствия в плане безопасности могут быть весьма серьезными. Технология может использоваться для манипулирования или контроля над поведением человека, что усиливает необходимость соблюдения строгих этических норм и мер защиты¹¹.

32. Беспилотные летательные аппараты самолетного и вертолетного типов используются для наблюдения за посевами и скотом, а также для внесения питательных веществ и пестицидов на посевы интеллектуальным и эффективным способом, позволяющим добиться максимальной продуктивности. В правоохранительных органах разработаны полуавтономные беспилотники, способные распылять средства противодействия массовым беспорядками. Возможность злонамеренного применения сельскохозяйственных дронов и БЛА для борьбы с беспорядками в качестве носителей опасных веществ вызывает постоянную обеспокоенность, особенно по мере того, как они становятся все более доступными и получают широкое распространение.

33. Интеграция новых технологий ведет также к созданию инновационных методов лечения и противодействия биологическим и химическим угрозам, таких как противоядия от ядов и новые меры противодействия воздействию нервно-паралитических веществ¹². Такие разработки крайне важны для повышения устойчивости к потенциальным атакам и даже для их предотвращения.

Соответствующие межправительственные процессы, органы и документы

34. И Конвенция по биологическому оружию, и Конвенция по химическому оружию предусматривают проведение раз в пять лет конференций по рассмотрению их действия, на которых проводится обзор соответствующих научно-технических достижений. В ноябре-декабре 2022 года состоялась девятая обзорная конференция государств — участников Конвенции по биологическому оружию, а в мае 2023 года — пятая обзорная конференция государств — участников Конвенции по химическому оружию.

35. В обеих конвенциях предусмотрены механизмы более частого обзора соответствующих достижений в области науки и техники. В соответствии с мандатом, полученным от Конференции государств — участников Конвенции по химическому оружию, Генеральный директор Организации по запрещению химического оружия (ОЗХО) создал в структуре этой организации научно-консультативный совет. В 2023 году Совет провел свою тридцать седьмую сессию¹³, а созданная им временная рабочая группа по анализу биотоксинов завершила работу

¹¹ Miryam Naddaf, “Mind-reading devices are revealing the brain’s secrets”, *Nature*, vol. 626, No. 8000 (February 2024); Rachael Levy, Marisa Taylor and Akriti Sharma, “Elon Musk’s Neuralink wins FDA approval for human study of brain implants”, *Reuters*, 26 May 2023.

¹² Illia V. Kapitanov and others, “Sustainable ionic liquids-based molecular platforms for designing acetylcholinesterase reactivators” *Chemico-Biological Interactions*, vol. 385 (November 2023).

¹³ OPCW, “Report of the Scientific Advisory Board at its thirty-seventh session”, document SAB-37/1.

и выпустила доклад, посвященный завершению выполнения ее мандата¹⁴. Кроме того, Совет опубликовал всеобъемлющий научный доклад о достижениях в области науки и техники в поддержку пятой Конференции государств — участников Конвенции о запрещении химического оружия по рассмотрению действия Конвенции¹⁵. Помимо этого, ОЗХО открыла свой Химико-технологический центр, который обеспечит ей возможность вести исследовательскую деятельность, призванную поддерживать и укреплять режим проверки, а также организовывать учебные курсы и осуществлять другие мероприятия по наращиванию потенциала.

36. На девятой Конференции государств — участников Конвенции о биологическом оружии по рассмотрению действия Конвенции в 2022 году государства-участники договорились о создании рабочей группы по укреплению Конвенции. Мандат рабочей группы состоит в том, чтобы выявлять, изучать и разрабатывать конкретные и эффективные меры, включая возможные юридически обязательные меры, а также выносить рекомендации по укреплению и институционализации Конвенции. Мандат предусматривает также обсуждение научно-технических достижений, имеющих отношение к Конвенции, и рекомендаций по созданию механизма для обзора и оценки таких достижений и предоставление консультаций государствам-участникам. Обсуждение этих тем состоялось на второй сессии рабочей группы в августе 2023 года и будет продолжено в рамках межсессионной работы и будущих встреч перед десятой обзорной конференцией, которая состоится в 2027 году.

Е. Космические и аэрокосмические технологии

Ракетные технологии

37. Развитие новых технологий позволяет создавать новые и наращивать функции ракетных систем, которые все чаще применяются в качестве ударного оружия большой дальности в вооруженных конфликтах. Эти события имеют последствия для международного мира и безопасности и усилий по обеспечению разоружения, эффективного регулирования вооружений, нераспространения и соблюдения гуманитарных принципов.

Баллистические ракеты и артиллерийские ракеты

38. Все большее число государств используют различные технологические инновации, которые повышают точность наведения баллистических ракет и реактивных артиллерийских систем. Это позволило применять баллистические ракеты и артиллерийские ракеты большей дальности в качестве ударного оружия, в том числе в ходе текущих вооруженных конфликтов и других резонансных инцидентов. Некоторые негосударственные субъекты также смогли приобрести и применять баллистические ракеты и артиллерийские ракеты.

39. Эти технологические инновации обеспечили возможность разработки и испытания артиллерийских ракет большого калибра, что может свести на нет различия между артиллерийскими реактивными снарядами и баллистическими ракетами, способными нести ядерную боевую часть. Эта тенденция по-прежнему

¹⁴ OPCW, “Analysis of biotoxins: report of the Scientific Advisory Board’s temporary working group”, document SAB/REP/1/23.

¹⁵ OPCW, “Report by the Director-General: report of the Scientific Advisory Board on developments in science and technology to the Fifth Special Session of the Conference of the States Parties to Review the Operation of the Chemical Weapons Convention”, document RC-5/DG.1.

создает проблему для режимов, призванных сдерживать распространение баллистических ракет, способных нести ядерную боевую часть.

40. Такие события побуждают государства разрабатывать и приобретать средства противоракетной обороны, определенные виды которых могут усиливать напряженность и усугублять международную нестабильность вследствие несовпадения взглядов на соотношение между наступательными и оборонительными системами вооружений.

Гиперзвуковые планирующие боевые блоки

41. Некоторые государства продолжают также разрабатывать и принимать на вооружение ракеты с боевыми частями, способными осуществлять на гиперзвуковых скоростях планирование и маневрирование в атмосфере на большие расстояния благодаря аэродинамической подъемной силе. Гиперзвуковые планирующие боевые блоки могут обходить системы противоракетной обороны на маршевом участке и создавать трудности для перехвата на конечном участке полета благодаря своей маневренности или потому, что на конечном участке своей траектории они летят на высотах ниже горизонта обнаружения наземных РЛС на большем удалении от своих целей. Применения таких систем в вооруженных конфликтах еще не наблюдалось, и стратегические последствия до конца не выяснены. Тем не менее первое известное оснащение в 2019 году гиперзвуковым планирующим боевым блоком межконтинентальной баллистической ракеты вызвало опасения по поводу нового соперничества в сфере стратегических вооружений.

Гиперзвуковые летательные аппараты с силовой установкой

42. Государства и частные компании продолжают испытания гиперзвуковых прямоточных воздушно-реактивных двигателей, предназначенных — по крайней мере частично — для создания гиперзвуковых крылатых ракет, обладающих большей способностью уклоняться от систем противовоздушной обороны и противоракетных систем. Такие системы, находящиеся в стадии активной разработки, могут запускаться с помощью ракет-носителей наземного, морского и воздушного базирования и оснащаться обычными или, возможно, ядерными боеголовками.

Системы противоракетной обороны и противоспутниковые системы наземного базирования

43. Все большее число государств разрабатывает и приобретает противоракетные системы, в том числе в порядке реагирования на их применение в текущих вооруженных конфликтах. Все большее распространение получают системы «земля-воздух», перехватывающие цель в нижних слоях атмосферы. Широкое развертывание этих систем привело к тому, что все чаще приобретаются и применяются, в том числе для преодоления такой защиты, недорогостоящие беспилотники, оснащенные устройствами самоподрыва.

44. Государства продолжают разрабатывать, испытывать и размещать системы противоракетной обороны, предназначенные для заатмосферного поражения ракет на маршевом участке полета. Наиболее совершенные из этих систем фактически способны поражать спутники на низкой околоземной орбите. Государства продолжают также развертывать ракеты наземного базирования, которые, как сообщается, были специально разработаны для нанесения ударов по спутникам на низкой околоземной и геостационарной орбите.

Соответствующие межправительственные процессы, органы и документы

45. В период 2001–2008 годов Генеральная Ассамблея учреждала три группы правительственных экспертов по вопросу о ракетах во всех его аспектах (см. [A/57/229](#), [A/61/168](#) и [A/63/176](#)). Вопрос о ракетах по-прежнему фигурирует в повестке дня Первого комитета, хотя за период после принятия резолюции [63/55](#) Генеральной Ассамблеи по этому вопросу не было принято ни одной резолюции.

46. Существуют два межправительственных режима, предусматривающих добровольные меры, связанные с ракетными технологиями. Режим контроля за ракетными технологиями был учрежден в 1987 году с целью ограничить распространение баллистических ракет и других беспилотных средств доставки оружия массового уничтожения. Он насчитывает 35 членов. В соответствии с Гаагским кодексом поведения по предотвращению распространения баллистических ракет, который был принят в 2002 году, государства принимают на себя имеющие обязательную политическую силу обязательства проявлять максимальную сдержанность в отношении разработки, испытания и развертывания баллистических ракет и поддерживать меры обеспечения транспарентности в отношении политики, касающейся баллистических ракет и космических летательных аппаратов, а также их пусков. К Кодексу присоединилось в общей сложности 145 государств.

47. Вопрос о противоспутниковом оружии наземного базирования поднимался в различных органах Организации Объединенных Наций, занимающихся вопросами безопасности в космическом пространстве, в том числе в последнее время в Группе правительственных экспертов по дальнейшим практическим мерам по предотвращению гонки вооружений в космическом пространстве. В своей резолюции [77/41](#) Генеральная Ассамблея призвала все государства не проводить испытаний противоспутниковых ракет прямого перехвата.

Космические технологии

48. При решении таких важных задач, как раннее предупреждение, навигация, наблюдение, целеуказание и связь, вооруженные силы во все большей степени опираются на космические технологии. Космические системы, включая спутники, особенно уязвимы для различных противокосмических средств.

Возможности, задействуемые в операциях сближения и маневрирования на близком расстоянии

49. Многие новые возможности связаны с операциями сближения и маневрирования на близком расстоянии, в которых участвуют спутники, маневрирующие вблизи спутника-цели, с тем чтобы действовать рядом или войти в физический контакт. Помимо полезного применения, например для обслуживания и ремонта спутников, такие операции могут использоваться и для совершения несогласованных, рискованных, подрывных или враждебных действий.

50. Продолжается разработка систем, способных оказывать другие услуги действующим спутникам на орбите, включая осмотр, ремонт, корректировка орбиты и перемещение. Коммерческие компании впервые продемонстрировали в 2020 году запуск спутника, способного пристыковаться к целевому спутнику, исчерпавшему запас топлива, и продлить его функционирование.

51. Все больше коммерческих компаний развертывают так называемые космические буксиры, предназначенные для вывода нескольких полезных нагрузок на точные орбиты в разных плоскостях и на разных высотах. Эти системы предназначены для маневрирования после вывода на орбиту и развертывания

множества малых спутников в различных точках на всем протяжении своих траекторий. Наблюдалось развертывание небольших дополнительных полезных нагрузок с помощью некоторых спутников на относительно высоких скоростях.

52. Коммерческие компании продолжают запускать демонстрационные спутники в поддержку развития возможностей активного удаления космического мусора. Эти компании продолжают изучать различные средства, включая использование дистанционных манипуляторов, сетей, гарпунов, магнитов и адгезивов, а также возможное применение лазеров космического базирования для уничтожения космического мусора относительно небольшого размера.

53. Ряд государств продолжает запускать и эксплуатировать спутники, предназначенные для визуального наблюдения за чужими спутниками, особенно на геостационарной орбите. Как правило, речь идет о системах, эксплуатируемых военными или национальными разведывательными службами, которые наблюдают как за коммерческими, так и другими военными спутниками.

Другие космические возможности

54. Коммерческие компании также продемонстрировали возможность установки теплозащитных экранов на полезную нагрузку своих спутников для получения материалов, которые были изготовлены на орбите. Коммерческие компании недавно разработали и используют системы возвращения в плотные слои атмосферы пилотируемых космических кораблей, хотя государства используют такие технологии уже несколько десятилетий.

55. Государства и коммерческие компании продолжают изучать и испытывать космические лазеры в качестве средств связи. В то время как лазеры малой мощности способны ослеплять или временно выводить из строя оптические датчики, более мощные лазеры могут повреждать некоторые чувствительные компоненты спутников и других космических систем.

Соответствующие межправительственные процессы, органы и документы

56. Международное право запрещает размещение и установку ядерного оружия или любого другого оружия массового уничтожения на орбите или на небесных телах, равно как и размещение такого оружия в космическом пространстве любым другим способом; создание на небесных телах военных баз, сооружений и укреплений, испытание любых типов оружия и проведение военных маневров; и любые испытательные взрывы ядерного оружия или любые другие ядерные взрывы в космическом пространстве¹⁶.

57. Вопрос о предотвращении гонки вооружений в космическом пространстве стоит на повестке дня Конференции по разоружению с 1985 года.

58. В 2013 году Группа правительственных экспертов по мерам транспарентности и укрепления доверия в космосе утвердила консенсусный доклад (A/68/189). В 2023 году Комиссия по разоружению согласовала рекомендацию о практическом выполнении рекомендаций, содержащихся в докладе Группы (см. A/78/42). В 2019 году Комитет по использованию космического пространства в мирных целях принял преамбулу и 21 руководящий принцип обеспечения долгосрочной устойчивости космической деятельности (A/AC.105/C.1/L.366) и впоследствии вновь учредил Рабочую группу по

¹⁶ Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела, статья IV; Договор о запрещении испытаний ядерного оружия в атмосфере, в космическом пространстве и под водой, подпункт а) пункта 1 статьи I.

долгосрочной устойчивости космической деятельности Научно-технического подкомитета с пятилетним планом, который начал претворяться в жизнь в 2021 году.

59. По просьбе Генеральной Ассамблеи в последние годы Генеральный секретарь создал две группы правительственных экспертов по дальнейшим практическим мерам предотвращения гонки вооружений в космическом пространстве. Группа, учрежденная в соответствии с резолюцией [72/250](#), собиралась в 2018 и 2019 годах, но в итоге не смогла утвердить доклад по вопросам существа (см. [A/74/77](#)). Группа, сформированная в соответствии с резолюцией [77/250](#), приступила к работе в 2023 году и представит доклад Ассамблее на ее семьдесят девятой сессии. В своей резолюции [78/238](#) Ассамблея постановила учредить рабочую группу открытого состава по этому пункту, которая будет проводить свои заседания в период с 2024 по 2028 год.

60. Своей резолюцией [76/231](#) Генеральная Ассамблея учредила рабочую группу открытого состава по уменьшению космических угроз путем принятия норм, правил и принципов ответственного поведения, которая собиралась в 2022 и 2023 годах. Рабочая группа не смогла утвердить доклад; однако мнения государств-членов были обобщены в рабочем документе, представленном Председателем ([A/AC.294/2023/WP.22](#)). Своей резолюцией [78/20](#) Ассамблея постановила учредить рабочую группу открытого состава по этому пункту, которая будет проводить свои заседания в период 2025–2026 годов.

Г. Электромагнитные технологии

61. Существует или разрабатывается целый ряд оружейных технологий, использующих электромагнитную энергию для достижения основной цели или для придания ускорения метательному снаряду. Это оружие можно разделить на три общие категории: а) средства радиоэлектронной борьбы, которые подавляют, блокируют или уничтожают потенциал противника в плане доступа к электромагнитному спектру; б) оружие направленной энергии, которое использует электромагнитную энергию для нанесения физических повреждений или разрушения; в) боевые электромагнитные ускорители, использующие электромагнитную энергию для разгона твердого снаряда до высокой скорости.

62. В современных военных системах зачастую применяются датчики, системы наведения и средства связи, использующие электромагнитные сигналы. Системы радиоэлектронной борьбы могут применяться для атаки на приводимые в действие электромагнитными сигналами военно-технические средства или для защиты собственных сил и средств. Одним из последних достижений является применение систем радиоэлектронной борьбы для нарушения связи между беспилотными летательными аппаратами и их наземными станциями, чему противодействует обеспечение все большей автономности таких систем. Ряд государств создают системы радиоэлектронной борьбы наземного базирования, предназначенные для нарушения работы спутниковых систем. Такой потенциал уже используется для создания помех в работе спутниковых систем, обеспечивающих вещание, геолокацию, навигацию и определение времени. С помощью систем радиоэлектронной борьбы можно обеспечить — особенно в мирное время — крупномасштабное нарушение или блокирование цифровой связи, например путем препятствования активными радиопомехами работе спутников, обеспечивающих доступ к интернету, и наземных станций управления ими.

63. Оружие направленной энергии включает в себя лазеры, высокомоощное СВЧ-излучение, волны миллиметрового диапазона и пучковое оружие. Государства с успехом испытывали лазеры наземного базирования против воздушных целей и разрабатывают такие системы для применения против беспилотных летательных аппаратов, ракет, снарядов и подлетающих боеприпасов. Одним из предполагаемых преимуществ таких систем является характерная для них низкая «стоимость одного выстрела». Судя по сообщениям, государства также применяли лазеры наземного базирования для подавления, ослепления или потенциального вывода из строя оптических датчиков спутников наблюдения на околоземной орбите. Продолжаются исследования, касающиеся применения систем, состоящих из множества волоконных лазеров весьма малого размера и лазеров на свободных электронах, в качестве оружия направленной энергии и электромагнитных импульсов в качестве противоспутникового оружия.

64. Оружие, в котором используется электромагнитный ускоритель, например рельсотрон или пушка Гаусса, способно запускать снаряды на большие расстояния и придавать им скорость, превышающую скорость, обеспечиваемую химическим топливом. Несмотря на проведенные огневые испытания прототипов таких средств, сохраняется ряд технических препятствий, включая потребность в мощном источнике энергии и достаточно прочных компонентах. Такое оружие в первую очередь предназначено для ограничения/воспреещения доступа и обороны на море.

Соответствующие межправительственные процессы, органы и документы

65. Вопросы, касающиеся средств ведения радиоэлектронной борьбы и оружия направленной энергии, рассматривались Группой правительственных экспертов по дальнейшим практическим мерам по предотвращению гонки вооружений в космическом пространстве (см. [A/74/77](#)). С текущими мнениями государств-членов можно ознакомиться в недавно опубликованных докладах Генерального секретаря, посвященных разоруженческим аспектам в космосе, включая документы [A/76/77](#) и [A/77/80](#). Рабочая группа открытого состава по уменьшению космических угроз путем принятия норм, правил и принципов ответственного поведения обсуждала вопросы, касающиеся радиоэлектронной борьбы, в рамках своего мандата, что нашло свое отражение в резюме Председателя ([A/AC.294/2023/WP.22](#)).

G. Технологии материалов

66. Прогресс в области материаловедения играет ключевую роль в применении инновационных подходов во многих сферах, имеющих отношение к обеспечению мира и безопасности. Так, например, новые виды материалов позволили добиться значительных успехов в усилиях по миниатюризации, снижению веса, повышению энергоэффективности, усилению защиты и прочности и снижению уровня радиолокационной заметности. Эти качества играют роль ключевых факторов, способствующих созданию современных платформ — носителей обычных вооружений, а также оружейных систем, их составных частей и компонентов.

67. Аддитивные технологии продолжают вносить революционные изменения в производственные процессы, обеспечивая децентрализацию процесса производства все более широкой номенклатуры составных частей и компонентов и тем самым еще более затрудняя экспортный контроль и процедуры управления цепочками поставок и их отслеживания. Совершенствование как промышленных, так и коммерческих принтеров, обеспечение способности использовать все

более широкий ассортимент материалов — даже в одном и том же устройстве — и наличие огромного массива знаний в открытых источниках способствовали еще большему снижению барьеров, препятствующих государственным и негосударственным субъектам создавать сложные компоненты для широкого применения в различных системах обычных вооружений и оружия массового уничтожения. В последние годы вызывает озабоченность межрегиональное распространение и повышение долговечности автоматического стрелкового оружия, изготовленного с помощью аддитивных технологий. Еще одна тенденция последнего времени — использование аддитивных производственных процессов для изготовления боеприпасов, в том числе малокалиберных; хотя в настоящее время они все еще менее эффективны, чем боеприпасы, изготовленные на обычном производстве, это создает дополнительные проблемы для контроля над стрелковым оружием и боеприпасами. Аддитивные технологии повысили также значимость неосязаемой передачи технологий и компьютерных разработок в контексте контроля над вооружениями.

68. Достижения в сфере нанотехнологий облегчили производство, транспорт и доставку химических и биологических агентов, что потенциально затрудняет усилия по обеспечению нераспространения. Продолжается разработка датчиков, в которых используются нанотехнологии. Такие датчики могут использоваться для обнаружения весьма небольших концентраций газов и паров. Эти достижения могут принести пользу в контексте усилий по контролю за разоружением. К рискам в сфере нанотехнологий относится токсичность и экологическая опасность некоторых наночастиц¹⁷. Нанотехнологии могут также способствовать развитию вычислительной техники и передовых средств связи для военных операций.

69. Оружие модульной конструкции состоит из множества компонентов, конфигурация которых может меняться. Такая модульность создает особые проблемы для выполнения предусмотренного в Международном документе, позволяющем государствам своевременно и надежно выявлять и отслеживать незаконные стрелковое оружие и легкие вооружения, требования о нанесении индивидуальной маркировки на основной или конструкционный элемент оружия. Кроме того, вызывает озабоченность использование полимерных пластмасс при производстве оружия, поскольку маркировку, нанесенную на такой материал, легче удалить или изменить по сравнению с маркировкой, наносимой на более традиционные материалы, такие как сталь.

Соответствующие межправительственные процессы, органы и документы

70. В своей резолюции 2325 (2016) Совет Безопасности просил Комитет, учрежденный резолюцией 1540 (2004), принимать к сведению в своей работе, когда это уместно, постоянно меняющийся характер рисков распространения, включая использование негосударственными субъектами стремительного прогресса в области науки, техники и международной торговли для целей распространения, в контексте осуществления резолюции 1540 (2004). Совет призвал также государства, в соответствующих случаях, обеспечивать контроль за доступом к нематериальной передаче технологий и информации, которые могут быть использованы для создания оружия массового уничтожения и средств его доставки.

¹⁷ UNIDIR, “Enabling technologies and international security: a compendium – 2023 edition”, 6 March 2024, pp. 13–15.

71. Генеральная Ассамблея рекомендовала государствам учитывать новшества, связанные с изготовлением, технологией производства и проектированием стрелкового оружия и легких вооружений, в частности оружия, изготовленного из полимеров, и оружия модульной конструкции, (см. резолюцию 78/46 Ассамблеи). В июне 2024 года четвертая Конференция Организации Объединенных Наций для обзора прогресса, достигнутого в осуществлении Программы действий по предотвращению и искоренению незаконной торговли стрелковым оружием и легкими вооружениями во всех ее аспектах и борьбе с ней, постановила учредить техническую группу экспертов открытого состава, которая соберется в течение недели после созываемых раз в два года совещаний государств в 2026 и 2028 годах, для разработки рекомендаций на основе консенсуса по обеспечению осуществления Международного документа по отслеживанию и Программы действий с учетом последних изменений в области изготовления, технологии производства и конструкции стрелкового оружия и легких вооружений, в частности оружия, изготовленного из полимеров, и оружия модульной конструкции, а также огнестрельного оружия, изготовленного посредством 3D-печати. Группа будет рассматривать как вызовы, так и возможности, возникающие в связи с развитием технологий. Кроме того, государства договорились содействовать передаче технологий маркирования, учета и отслеживания стрелкового оружия и легких вооружений, обмениваться практическими методами борьбы с незаконным изготовлением с использованием технологий аддитивного производства и сообразно обстоятельствам взаимодействовать с отраслью аддитивного производства (см. [A/CONF.192/2024/RC/3](#)).

III. Конвергенция технологий

72. Конвергенция науки и технологий подразумевает междисциплинарное взаимодействие конкретной технологической области с новейшими и уже существующими технологиями. Такая конвергенция создает как возможности, так и вызовы в контексте международного мира и безопасности. Результатом междисциплинарного взаимодействия зачастую являются инновации и прорывы в науке. С одной стороны, стремительный научно-технический прогресс может способствовать развитию человеческого потенциала и служить катализатором реализации Повестки дня в области устойчивого развития на период до 2030 года. С другой стороны, взаимодействие этих технологий может повлечь за собой неожиданные последствия для международного мира и безопасности.

73. Данные являются строительными блоками для развития технологий и лежат в основе усиливающегося взаимодействия между несколькими технологическими областями. В настоящем разделе представлен обзор вызывающих озабоченность вопросов, которые часто поднимают участники многосторонних обсуждений.

Искусственный интеллект и автономность

74. Искусственный интеллект не является обязательным условием для функционирования автономных систем вооружений. Однако его применение может способствовать еще большему повышению автономности.

75. Некоторые из потенциальных применений искусственного интеллекта в контексте автономных систем вооружений включают: а) обработку в режиме, близком к реальному времени, данных, получаемых с помощью различных датчиков (от наземных РЛС до спутников) и электронных сигналов для распознавания, идентификации и классификации целей; б) автономную навигацию в различных условиях местности и адаптацию к ним по времени производства

выстрела из оружия и времени подрыва; с) анализ угроз в режиме реального времени и выбор курса действий или предоставление возможности выбора действий человеку-оператору; d) извлечение уроков из практики выполнения предыдущих задач и прошлых столкновений для улучшения работы с течением времени; и е) использование обработки естественного языка и компьютерного зрения для обеспечения взаимодействия человека и машины.

76. Одним из вызовов, связанных с использованием искусственного интеллекта в военной сфере и автономностью, является понятие «контроля со стороны человека» над применением силы¹⁸. Многие государства и неправительственные эксперты ставят под сомнение приемлемые уровни автономности важнейших функций систем вооружений, включая выбор цели и применение силы к целям.

77. В рамках Группы правительственных экспертов по новейшим технологиям в сфере смертоносных автономных систем вооружений, сформированной под эгидой Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие, многие государства отмечали, что системы оружия, функционирующие полностью без «контроля со стороны человека», не могут являться приемлемыми с правовой и этической точек зрения. Остаются разногласия по поводу необходимой степени «контроля со стороны человека» на различных этапах «жизненного цикла» системы¹⁹. Различаются мнения и по вопросу о том, необходим ли «контроль со стороны человека» для соблюдения норм международного гуманитарного права.

ИКТ, искусственный интеллект и квантовые технологии

78. Функционал искусственного интеллекта может создавать как риски, так и благоприятные возможности для безопасности в сфере ИКТ.

79. Государства и частные компании все чаще используют искусственный интеллект для обнаружения потенциальных угроз в своих ИКТ-сетях. Так, системы с искусственным интеллектом могут автоматически обнаруживать и блокировать попытки фишинга, вредоносные программы и другие злонамеренные действия на основе анализа нетипичных явлений и аномалий в сетевом трафике.

80. В то же время искусственный интеллект может создавать и риски в сфере ИКТ. Приложения искусственного интеллекта, такие как большие языковые модели, могут использоваться злоумышленниками для создания вредоносных кодов, выявления уязвимостей на уровне системы, распространения ложной информации или взлома существующих методов шифрования. Хотя эти риски не являются уникальными для больших языковых моделей или генеративного искусственного интеллекта, они могут усиливаться ими²⁰. Искусственный интеллект может создавать «дипфейки» — реалистичные, но полностью вымышленные видеоролики, в том числе с участием общественных деятелей, распространяющие ложную информацию и влияющие на общественное мнение. Кроме

¹⁸ В настоящее время у государств не имеется согласованной терминологии применительно к контролю со стороны человека. Также используются такие термины, как конструктивный контроль со стороны человека, вмешательство человека, надзор со стороны человека, соответствующее оценочное суждение человека, участие человека и включение/выключение человека в/из контур(а) управления.

¹⁹ Жизненный цикл искусственного интеллекта включает в себя несколько этапов, в том числе предварительное и рабочее проектирование, разработку, ввод в эксплуатацию, эксплуатацию и вывод из эксплуатации, но не ограничивается ими.

²⁰ Ioana Puscas, *AI and International Security: Understanding the Risks and Paving the Path for Confidence-building Measures* (Geneva, UNIDIR, 2023).

того, злоумышленники могут создавать дипфейки, имитирующие голоса родных и близких²¹.

81. Модели искусственного интеллекта могут стать объектом злонамеренной деятельности в сфере ИКТ, когда злоумышленники используют модели искусственного интеллекта для получения доступа к исходным кодам или наборам данных или для преднамеренного вброса ложных или вводящих в заблуждение данных в наборы обучающих данных. Последнее явление, известное как отравление данных, подрывает безопасность и надежность пользования системами искусственного интеллекта.

82. Квантовые технологии в сочетании с другими технологическими приложениями, такими как ИКТ и искусственный интеллект, могут создавать как возможности, так и вызовы в сфере мира и безопасности. Ожидается, что технология квантового распределения ключей позволит обеспечивать безопасную связь между сторонами. Квантовое распределение ключей может также обеспечивать более эффективное шифрование и дешифрование данных, что необходимо для безопасности цифровых средств. Ожидается, что квантовые технологии позволят также усовершенствовать протоколы безопасности ИКТ на основе квантовых принципов. Однако с развитием вычислительной мощности квантовые компьютеры способны взламывать широко используемые методы шифрования, создавая угрозу для существующих криптографических систем. Это может привести к появлению новых уязвимостей, в том числе в случае критически важной инфраструктуры, используемой для предоставления основных услуг населению. Интеграция квантовых технологий в ИКТ, вероятно, создаст дополнительные вызовы для стран с ограниченными возможностями, что потребует создания специального потенциала в этой области, например путем решения вопросов глобального доступа к квантовым технологиям и формирования в мировом масштабе кадров, обладающих квантовой грамотностью.

83. Рабочая группа открытого состава по безопасности информационно-коммуникационных технологий и их безопасному использованию в 2021–2025 годах предоставляет государствам-членам возможность обмена мнениями о существующих и потенциальных угрозах. В ее рамках многие государства-члены обращают особое внимание на риски и возможности, создаваемые искусственным интеллектом и квантовыми технологиями, в числе прочих технологий, в связи с ИКТ.

Искусственный интеллект и науки о жизни

84. Как отметил Генеральный секретарь в концептуальной записке, посвященной «Новой повестке дня для мира», многочисленные технологии, связанные с науками о жизни, развиваются и конвергируются, создавая значительные потенциальные выгоды для общества в целом. Конвергенция наук о жизни с приложениями искусственного интеллекта позволяет накапливать и анализировать огромные объемы данных в целях выявления закономерностей, благодаря чему появляется возможность эффективнее решать проблемы в сфере здравоохранения.

85. Вместе с тем такие достижения могут также снижать стоимость и технические барьеры на пути разработки биологического оружия. Приложения искусственного интеллекта могут использоваться для разработки, синтеза и распространения опасных биологических веществ или для создания систем доставки, что позволит получить новое, усовершенствованное биологическое оружие.

²¹ Emily Flitter and Stacy Cowley, “Voice deepfakes are coming for your bank balance”, *The New York Times*, 30 August 2023.

Другие каскадные последствия слияния искусственного интеллекта и биологии могут включать в себя искусственно вызываемые пандемии или другие непредвиденные события.

86. Интеграция генеративного искусственного интеллекта в конструирование белков и открытие лекарств стремительно меняет подходы к решению проблем здравоохранения, позволяя ученым и разработчикам ускорять процесс прогнозирования функционирования новых белков и малых молекул, а также их взаимодействия с другими молекулами. Такая точность может произвести революцию в фармацевтических исследованиях и разработках, но при этом вызывает серьезные опасения по поводу двойного назначения²². Достижения в области конструирования белков и других молекул способны повышать вирулентность или устойчивость патогенов, что вызывает опасения по поводу их возможного применения в качестве биологического оружия. Потенциальное применение в этих злонамеренных целях подчеркивает настоятельную необходимость международного диалога и сотрудничества для обеспечения ответственного использования таких технологий.

87. Применение автоматизированного или полуавтоматизированного химического синтеза, при котором роботизированные платформы на базе генеративного искусственного интеллекта помогают выполнять операции синтеза или полностью выполняют их, открывает перспективу рационализации производства химических веществ, потенциально снижая затраты, время исполнения и сложность операций. Полностью автоматизированные системы могут даже способствовать снижению барьеров для использования, позволяя неспециалистам выполнять сложные химические превращения. Это может стимулировать инновации, но при этом также повышается вероятность скрытого производства опасных веществ. Это создает серьезные вызовы в сфере международного мира и безопасности, поскольку может способствовать распространению отравляющих веществ и усложнить надзор и мониторинг опасных веществ.

Науки о жизни и ИКТ

88. Конвергенция биологии и ИКТ²³ коренным образом повлияла на характер исследований в области наук о жизни, создав новые возможности для сотрудничества и ускорения исследований, например благодаря расширению доступа к наборам данных. Однако такая конвергенция может создавать и значительные риски, включая эксплуатацию уязвимостей сетей в сфере здравоохранения, в том числе в медицинских центрах и биологических лабораториях, а также в производственно-сбытовых цепочках²⁴. Кроме того, существуют опасения по поводу возможного манипулирования данными исследований и несанкционированного доступа к ним, которые могут привести к разглашению конфиденциальной медицинской информации. Это может подорвать доверие населения к учреждениям здравоохранения, затруднять усилия по борьбе с глобальными пандемиями и усиливать напряженность в отношениях между государствами в части соблюдения норм безопасности в сфере ИКТ.

²² См. <https://www.nature.com/articles/d41586-024-00699-0>, <https://www.technologyreview.com/2023/02/15/1067904/ai-automation-drug-development/>, <https://communities.springernature.com/posts/cavitomix-drug-solver-a-gpu-accelerated-tool-for-drug-repurposing-and-off-target-analysis-using-cavity-property-point-clouds-on-nvidia-dgx-a71725f0-77f6-46e5-8a3d-9c6d19aae6b6> и <https://www.nvidia.com/en-us/clara/bionemo/>.

²³ См.: https://documents.unoda.org/wp-content/uploads/2021/04/07_31_Pauwels_Slides_MX2.pdf.

²⁴ Lauren C. Richardson and others, "Cyberbiosecurity: a call for cooperation in a new threat landscape", *Frontiers in Bioengineering and Biotechnology*, vol. 7 (June 2019).

Ядерное оружие, ИКТ и искусственный интеллект

89. Ядерное оружие появилось на свет, когда компьютерные технологии находились еще в зачаточном состоянии²⁵. В этой связи мало внимания уделялось потенциальным последствиям искусственного интеллекта и безопасности ИКТ, которые в настоящее время представляют собой явные потенциальные вызовы для ядерного оружия и связанных с ним систем оперативного управления и раннего предупреждения.

90. Вредоносная деятельность в сфере ИКТ в мирное время может усиливать напряженность и повышать вероятность возникновения вооруженных конфликтов с применением обычных видов оружия между государствами, обладающими ядерным оружием, тем самым увеличивая потенциал ядерной эскалации (см. A/76/182). Во время вооруженных конфликтов вредоносная деятельность в сфере ИКТ, направленная на системы ядерного оружия или системы двойного назначения, такие как системы раннего предупреждения, может привести к неправильному восприятию ситуации и просчетам, что потенциально может повлечь за собой непреднамеренное применение ядерного оружия.

91. Эксперты выявили такие виды деятельности, как хакерство, спуфинг, создание помех и другие злонамеренные действия, направленные на эксплуатацию потенциальных уязвимостей ИКТ в системах ядерного оружия. Эти уязвимости охватывают: а) связь между системами командования и управления²⁶; б) связь, осуществляемая с командных пунктов с ракетными пусковыми установками (например, подводными лодками) и ракетами; в) телеметрические данные с ракет, передаваемые на наземные и космические средства оперативного военного управления; г) аналитические центры для сбора и интерпретации данных; д) цифровые технологии на транспорте; е) использование цифровых технологий в лабораториях и на сборочных производствах; ж) информацию о целеуказании, получаемую в режиме реального времени от систем космического базирования, включая данные о местоположении, навигации и времени; з) данные о местоположении пусковых установок; и) информацию о целеуказании, получаемую в режиме реального времени с наземных станций; и) автономные системы или системы с искусственным интеллектом, интегрированные в систему командования, управления или связи.

92. Государства — участники Договора о нераспространении ядерного оружия индивидуально и группами выражали обеспокоенность по поводу связи между такими технологиями и ядерным оружием, в том числе в различных рабочих документах, представлявших в течение всего цикла рассмотрения действия Договора²⁷.

93. Интеграция искусственного интеллекта в ядерное оружие и потенциальные уязвимости ИКТ в системах командования, управления и связи ядерных сил потенциально могут подрывать международную стабильность и влиять на такие концепции безопасности, как взаимное сдерживание (там же). Злоумышленники могут использовать уязвимости ИКТ для совершения некинетических атак, например подмены или взлома систем раннего оповещения, чтобы вызвать ложные тревоги или нарушения сетевой безопасности, которые могут перерасти в непреднамеренную ядерную конфронтацию. Искусственный интеллект может

²⁵ См. <https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf>.

²⁶ UNIDIR, *Understanding Nuclear Weapon Risks*, John Borrie, Tim Caughley and Wilfred Wan, eds. (Geneva, 2017).

²⁷ См., например, NPT/CONF.2020/WP.6, NPT/CONF.2020/WP.9/Rev.1, NPT/CONF.2020/WP.70, NPT/CONF.2026/PC.I/WP.24 и NPT/CONF.2026/PC.I/WP.30.

повышать изощренность таких атак. Во время вооруженных конфликтов опасения по поводу вмешательства в функционирование систем ядерного оружия могут создавать дестабилизирующие условия, при которых государства будут считать себя вынужденными применить ядерное оружие первыми, что приведет к быстрой и неконтролируемой эскалации.

94. Интеграция искусственного интеллекта в системы ядерного оружия, как, например, автономное управление или предварительное делегирование полномочий на пуск ядерного средства, может привести к катастрофическим последствиям. Технические проблемы безопасности искусственного интеллекта, такие как отравление данных и принятие потенциально непредсказуемых решений («черный ящик»), вызывают особую озабоченность по поводу возможной достоверности информации, имеющей критически важное значение для принятия решений в ядерной сфере, и повышают вероятность непреднамеренного применения ядерного оружия²⁸. Использование искусственного интеллекта в системах командования, управления и связи в ядерных силах может привести к сжатию сроков принятия решений, когда скорость действий, совершаемых искусственным интеллектом, может опережать возможности человека, что повлечет за собой просчеты и эскалацию в кризисных ситуациях. Во избежание таких возможных последствий три государства, обладающие ядерным оружием, в своем рабочем документе для десятой Конференции участников Договора о нераспространении ядерного оружия по рассмотрению действия Договора (NPT/CONF.2020/WP.70) подчеркнули свою приверженность сохранению «человеческого контроля и участия применительно ко всем действиям, имеющим критически важное значение для информационного обеспечения и исполнения суверенных решений, касающихся применения ядерного оружия».

IV. Выводы и рекомендации

95. Структуры Организации Объединенных Наций будут и далее поддерживать и поощрять текущие и потенциальные новые процессы рассмотрения возникающих проблем, прежде чем эти проблемы перерастут в угрозу миру и безопасности, правам человека, гуманитарным нормам и принципам или иным целям и задачам Организации. Государствам-членам рекомендуется определять многосторонние форумы, подходящие для обсуждения синергии технологий, рассмотренных в настоящем докладе.

96. Комиссия по разоружению постановила рассмотреть пункт повестки дня, озаглавленный «Рекомендации в отношении общего понимания новейших технологий в контексте международной безопасности», в ходе своего трехгодичного цикла 2024–2026 годов. Для государств-членов это является важной возможностью рассмотреть междисциплинарные соображения, применимые ко всем новейшим технологиям, а также принять к сведению те новейшие технологии, которые чреваты последствиями для международной безопасности, но в настоящее время не обсуждаются в рамках процессов Организации Объединенных Наций.

²⁸ В вычислительной технике «черный ящик» — это система, в отношении которой известны входные и выходные данные, но не процесс, с помощью которого система превращает первые во вторые. Это те случаи, когда внутреннее функционирование и процессы принятия решений в системе искусственного интеллекта непрозрачны и не поддаются объяснению или пониманию человеком. См. <https://undir.org/files/2020-09/BlackBoxUnlocked.pdf>.

97. Органам и структурам Организации Объединенных Наций рекомендуется и далее поощрять многостороннее, основанное на принципе справедливой географической представленности и гендерно сбалансированное участие различных заинтересованных сторон, в том числе представителей научно-образовательного сообщества, промышленности и частного сектора, на формальных и неформальных площадках.

98. Государствам-членам рекомендуется продолжать изыскивать пути включения обзоров научно-технических достижений в свою работу в рамках всех соответствующих разоруженческих органов Организации Объединенных Наций, в том числе в рамках процессов рассмотрения действия договоров о разоружении. Это может повлечь за собой создание механизмов научно-технического обзора, когда это уместно, для информационного обеспечения межправительственных обсуждений. Такие механизмы обзора должны обеспечивать выявление и изучение новых и новейших технологий, которые способны закреплять или усиливать социальные предубеждения, в том числе гендерные, и их влияния на применение международного права.

99. Саммит будущего, который будет проходить 22–23 сентября 2024 года, предоставляет важную возможность принятия дальновидных и конкретных решений в отношении новейших технологий и их влияния на мир и безопасность. Я настоятельно призываю государства-члены принять меры в соответствии с рекомендациями, сформулированным в моей концептуальной записке, посвященной «Новой повестке дня для мира».

100. Генеральной Ассамблее рекомендуется и далее ежегодно запрашивать доклады с изложением обновлений к информации, содержащейся в настоящем докладе, в качестве вклада в поддержание осведомленности о научно-технических достижениях и их потенциальном воздействии на усилия в области международной безопасности и разоружения.