Текст · 28 апреля 2022, 07:34

Находка для шпиона. Как искусственный интеллект подслушивает российских военных в Украине

Одной из самых странных отличительных черт войны с Украиной стало обилие прослушек переговоров российских войск, публикуемых в СМИ и социальных сетях. Зашифрованной радиосвязи не оказалось у многих частей, а в отдельных случаях и у командования, поэтому на поле боя военным пришлось переговариваться на частотах, которые можно легко прослушать.

С разрешения *Wired* «Медиазона» публикует перевод материала о следующем шаге в использовании этой уязвимости — автоматическом анализе содержания радиоперехватов, которым занимается частная американская компания *Primer*.

Растерянные российские военные в панике отступают, попав под артиллерийский обстрел, и обмениваются короткими репликами по радиосвязи — по незащищенному каналу.

«Восток, я Снег-02. Нам на шоссе налево, бля», — говорит военный, используя позывные. «Я понял. Дальше и не надо. К обороне переходим. Прием», — получает он в ответ.

Позже еще один военный пытается связаться с сослуживцем: «Юг-95, есть [со старшим] связь?

Выйди на старшего, предупреди: на шоссе обстрел артиллерии. На шоссе обстрел артиллерии. В рамках колонны не выступать. Пускай аккуратно двигается. Пускай двигается аккуратно».

Далее он продолжает еще более взволнованным голосом: «Как слышите? Как обстановка и местонахождение артиллерии, предположительно из какого орудия [ведут стрельбу]?». И позже: «Обозначьте ваш сектор. Юг-95, отвечайте на мои вопросы. Обозначьте название своего сектора!».

Пока военные переговариваются, их слушает искусственный интеллект: их речь автоматически перехватывается, расшифровывается, переводится и анализируется при помощи сразу нескольких алгоритмов искусственного интеллекта американской компании *Primer*, которая разрабатывает решения для разведки. Мы не знаем, удается ли украинским войскам перехватывать тот же радиообмен собственными силами, но широкое использование систем искусственного интеллекта для наблюдения за действиями российской армии показывает, насколько полезной может быть разведка по открытым данным.

Перехваты радиообмена по незащищенным каналам связи публикуются в открытом доступе, переводятся на английский и анализируются. Столь же тщательно изучаются прочие данные, от видеозаписей со смартфонов до сообщений в соцсетях. Принципиальным новшеством стало использование технологий автоматической обработки речи, с помощью которых анализируется содержание

радиообмена между российскими военными. В украинской армии обработкой перехватов, как правило, занимаются живые люди, которые сидят где-то, расшифровывают и анализируют сообщения.

Фрагмент перехваченного радиообмена

Голос 1. Алмаз, я Буран, прием.
Голос 2. Как у тебя обстановка? Прием.
Голос 1. Алмаз, у меня обстановка пока спокойная, кроме самолетов и вертолета не было. На западной части района постоянно работает артиллерия. Артиллерия работает по Югу. Потерь нет. Снег-02 подвергся обстрелу, потерял три коробочки. Пять коробочек. Сгорели. По потерям уточняю. Я Буран, прием.
Голос 2. По людям есть потери?
Голос 1. По людям пока не готов, вызываю Снега. Прием.

Выжимка, подготовленная искусственным интеллектом

Алмаз срочно выходит на связь. Снег-02 находится в секторе 2 на перекрестке, попал под артиллерийский обстрел. Сгорели 4–5 танков. Алмаз позвонит старшему. Бритва, Алмаз, Снег и Буран движутся по дороге и находятся возле перекрестка. Бритва перейти на другую сторону дороги не готов.

Расшифровка одного из диалогов с записи перехвата российских военных и краткое описание ситуации в целом, подготовленное ИИ Primer

Успех *Primer* показывает ценность машинного обучения для анализа разведданных. За последнее десятилетие искусственный интеллект стал значительно лучше распознавать изображения, транскрибировать устную речь, переводить и анализировать содержание — благодаря нейронным сетям, которые тренируют на больших массивах данных. Уже имеющиеся на рынке программные решения могут покрыть запросы по расшифровке речи, распознаванию лиц и выполнению аналогичных задач с довольно высокой точностью. Перехват радиообмена может отчасти компенсировать численное превосходство российской армии и ее преимущество в военной технике.

Гражданским клиентам *Primer* предлагает алгоритмы искусственного интеллекта для анализа телефонных звонков, умеющие вычленять ключевые термины и фразы. Генеральный директор компании Шон Гурли говорит, что разработчики модифицировали эти инструменты для четырех новых задач: для захвата аудио из интернет-каналов, транслирующих перехваты, удаления шумов, в том числе фоновых разговоров и музыки, расшифровки и перевода русской речи и вычленения ключевых фраз, касающихся ситуации на поле боя. Для этого в том числе потребовалось переобучить модели машинного обучения, чтобы они понимали разговорные обозначения боевых машин и оружия, которые используются российскими военными.

Разработчики Primer рассказывают о механизме анализа радиоперехватов в подробном посте в своем блоге. Помимо технических деталей вроде захвата аудиостримов и шумоподавления и распознавания речи в сообщении рассказывается, как различные модели анализа речи суммируют содержание текста, вычленяют приказы, устанавливают упоминаемые виды оружия и составляют списки имен и географических названий, упоминаемых в перехвате.

«Всего один день работы с аудиофайлами дал оперативную информацию о том, что российские войска попали под интенсивный обстрел, теряют танки и получили приказ отступать со своих позиций», — рассказывают в Primer. Анализ передвижений войск ведется «практически в режиме реального времени»,

а автоматизация процесса позволяет «снять ограничения, связанные с необходимостью хорошо знать русский язык и часами слушать радиоэфир». В апреле компания выиграла крупный контракт на поставку решений для военно-воздушных сил США.

Гурли уверен, что возможность обучать и переучивать модели искусственного интеллекта на ходу даст армиям-участницам будущих войн ощутимое преимущество. Он добавляет, что доступ к программе открыли и для «третьих сторон», но не называет их. «Мы не будем раскрывать, кто и для чего эти алгоритмы использует», — подчеркивает он. Известно, что по ходу вторжения еще несколько других американских компаний начали делиться с украинской стороной своими технологиями, данными и навыками.

Зарубежных военных аналитиков шокировало использование некоторыми российскими частями незащищенных каналов связи. По словам специалиста по современным методам ведения войны Питера Сингера, старшего научного сотрудника аналитического центра *New America,* это свидетельствует о нехватке оборудования и неподготовленности самой операции.

«Российские военные раньше сами использовали перехваты переговоров по незащищенным каналам для наводки ударов по вражеским целям, например, в Чечне, так что уж им-то все риски должны были быть хорошо известны», — говорит Сингер. Он добавляет, что украинцы могли получить

преимущество благодаря перехватам, даже если анализ данных проводился вручную.

«Это говорит о технических сбоях в оборудовании [для шифрованной связи], некоторой самонадеянности российских военных и, возможно, об уровне отчаяния среди военного командования», — добавляет австралийский генерал в отставке Мик Райан.

По мнению Колдера Уолтона, историка шпионажа из Гарвардского университета, развитие событий в Украине подчеркивает ценность информации из открытых источников для разведок. Он отмечает, что алгоритмы для распознавания лиц уже используются для идентификации людей на видео военного времени. «Наступает абсолютно новая эпоха в части сбора разведданных и их доступности», — считает Уолтон.

Война в Украине подсветила и важность поиска различных источников разведывательной информации, говорит он. Так, по некоторым сообщениям, число погибших российских генералов может объясняться тем, что украинские военные охотятся на седовласых мужчин, которых видят на спутниковых снимках рядом с антеннами, на фотографиях с беспилотников и прочих изображениях. Российские военнослужащие часто используют мобильные телефоны, временами выдавая свое местонахождение и даже боевые задачи, и раскрывают данные об общем уровне деморализации.

Уолтон уверен, что Агентство национальной безопасности США *(NSA)* и их британские коллеги из Центра правительственной связи *(GCHQ)* располагают инструментарием, аналогичным тому, который используют в *Primer*, но важно и то, что число таких компаний растет, и технологии становятся все более и более доступными для военных и частного бизнеса. При этом вовлеченность частных компаний в военный конфликт — например, тех, что предоставляют услуги спутниковой связи и спутниковые снимки, — поднимает вопрос о том, какую ответственность они несут в ситуации, когда есть реальная опасность международного конфликта.

Сбор разведданных по открытым источникам требует просеивания большого количества информации. «Такие объемы никому не под силу охватить целиком», — говорит Эмили Хардинг, старший научный сотрудник организации *Center for Strategic and International Studies*-, некоммерческой организации, занимающейся политическими исследованиями (в январе 2022 года у нее вышел доклад на эту тему). Хардинг говорит, что разведсообщество уже далеко продвинулось в анализе изображений с помощью инструментов машинного обучения, это был первый шаг в использовании современных ИИ-разработок. Теперь же, говорит Хардинг, появились разработки вроде *Primer,* которые отличаются высоким качеством распознавания речи.

Успех разработок в области искусственного интеллекта привел к появлению мощных инструментов по анализу текста и речи.
С появлением трансформеров[1] ИИ научился

вычленять главное из текста или отвечать на вопросы. Трансформеры лежат в основе программ, генерирующих связные новостные заметки или даже пишущих программный код под конкретные задачи.

Впрочем, отмечает Хардинг, при работе с искусственным интеллектом разведкам придется столкнуться с теми же проблемами, которые мешают внедрению этих алгоритмов в других сферах — например, с их «предвзятостью», обусловленной низким качеством или нерепрезентативностью входных данных. «Хлам на входе — хлам на выходе», — говорит она. А поскольку прозрачность алгоритмов машинного обучения зачастую оставляет желать лучшего, разведкам придется искать способы оптимизации программ таким образом, чтобы их выдаче можно было доверять. Неправильно расшифрованное сообщение может иметь фатальные последствия на поле боя — например, отправить солдат по опасному маршруту или неверно направить ракетный удар.

Американские военные вкладывают миллионы в разработку ИИ, способного принимать и анализировать различные сигналы в полевых условиях. Программа армии США под названием *TITAN*[2] предполагает создание единого пункта по сбору и анализу информации с множества различных источников на поле боя. Если вторжение России в Украину проходит по привычным сценариям — танковые атаки и артобстрелы, — то будущие войны, к которым готовятся США и другие страны, могут в значительной степени опираться на новые технологии, в том числе ИИ.

Хотя такие разработки могут дать военным серьезное преимущество, специалисты предупреждают, что в соперничество за превосходство по искусственному интеллекту могут влючиться обе противоборствующие стороны, и тогда на первое место выйдут умения обманывать и запутывать алгоритмы. «Мы твердо убеждены: с каким алгоритмом ни начинай войну, закончишь ее с совершенно другим», — рассуждает Гурли из *Primer.*

Автор: Уилл Найт.

Оригинал: *"As Russia Plots Its Next Move, an AI Listens to the Chatter"; Wired, April 4, 2022.*

Перевод: Ксения Манукян

---

1. Сравнительно новый тип архитектуры нейронных сетей, который позволяет анализировать весь текст сразу, а не пословно, что положительно сказывается на понимании алгоритмом контекста.

2. Дословно «Узел доступа к тактическим разведывательным целям»