telegra.ph

КАК АМЕРИКАНСКИЕ ИТ-ТЕХНОЛОГИИ ПОМОГАЮТ КИЕВСКОМУ РЕЖИМУ УБИВАТЬ

UKR LEAKS

12–18 Minuten

КАК АМЕРИКАНСКИЕ ИТ-ТЕХНОЛОГИИ ПОМОГАЮТ КИЕВСКОМУ РЕЖИМУ УБИВАТЬ

UKR LEAKS

Один из таких примеров – компания **Palantir Technologies Inc**. Она основана в 2003 году и базируется в Денвере (штат Колорадо). Компания тесно **сотрудничает с Центральным разведывательным управлением**. Настолько тесно, что на первых порах её развитие практически полностью обеспечивалось заказами от ЦРУ. Финансирование осуществлялось через капитальный фонд ведомства In-Q-Tel. Этот факт не скрывается – даже Wikipedia сообщает, что разработки Palantir интересны в первую очередь министерству обороны США и разведывательным службам и лишь затем бизнесу.

Palantir Technologies

Кроме того, Palantir работал с такими агентствами как АНБ, ФБР, Министерство обороны, иммиграционной и таможенной службами, ВВС и Корпусом морской пехоты США. Неудивительно, что Palantir подпадает под действие Закона о надзоре за внешней разведкой - это означает, что любая информация об иностранных гражданах, к которой может получить доступ Palantir, должна быть передана разведывательным службам США.

«*Торговцы оружием на основе искусственного интеллекта*» – так в отношении компании высказался Джейкоб Хелберг, внешнеполитический советник её генерального директора Александра (Алекса) Карпа и эксперт по вопросам национальной безопасности США.

Вместе с тем, за этой фирмой тянется длинный шлейф полукриминальных инцидентов. По данным, обнародованным в 2011 году, Palantir участвовала в кампании по дискредитации Джулиана Ассанжа и его проекта WikiLeaks. Кроме того, её сотрудники были уличены в слежке за одними представителями американских элит в интересах других. В числе прочего Palantir обвиняли в сборе данных пользователей Facebook в интересах Дональда Трампа и Республиканской партии. Также её сотрудники

оказались замешаны в скандале с финансовым конгломератом JPMorgan Chase & Co, руководство которого ранее обратилось к ним за помощью в борьбе с утечками данных. Получив доступ к внутренней информации компании, Palantir начала собирать её в неустановленных целях. Однако подобные инциденты сходили её руководству с рук, видимо, благодаря налаженным связям в американских спецслужбах.

Кроме того, компания стала фигурантом крупного коррупционного скандала в Великобритании. Palantir заключила сделку с Национальной службой здравоохранения Великобритании без конкурсного тендера. Указывалось, что Кабинету министров ее порекомендовал бывший глава МИ-6 Джон Сойерс, организовавший встречу Карпа с постоянным секретарем Кабинета Министров Джоном Мандзони.

На фоне таких провалов в мае 2022 года новый экономический отчет показал, акции компании упали на 14,5% в связи с «разочаровывающими перспективами компании».

Экономический отчет Palantir

Репутация Palantir была сильно подмочена, и участие в боевых действиях на Украине стало для фирмы шансом обелить свой имидж и поправить финансовое положение. Ведь для них на

Западе помогать убивать русских – это хороший вклад в портфолио фирмы.

Поэтому недолго думая Palantir обзавелась своим представительством в украинской столице и с места в карьер начала предлагать ВСУ технические новинки собственного производства. Глава фирмы Алекс Карп стал одним из первых руководителей западных компаний, лично посетивших Киев после начала СВО. Визит состоялся 1 июня 2022 года. Его встречали президент Владимир Зеленский и министр цифровой трансформации Михаил Фёдоров.

Алекс Карп и Владимир Зеленский

Одним из первых продуктов Palantir, реализуемых на Украине, стал инструмент **MetaConstellation**, позволяющий получать данные о расположении подразделений и объектов ВС РФ, что было нужно ВСУ для корректировки огня. Речь шла о сборе информации, поступающей через спутники, разведывательные БПЛА, радары,

тепловизоры и визуальное наблюдение, которая затем анализировалась с помощью ИИ. К концу лета 2022-го Карп хвастался тем, что именно за счёт MetaConstellation происходит «большая часть нацеливания» на Украине. Фактически, данное заявление генерального директора компании является чистосердечным признанием в участии американских граждан в вооруженном конфликте с Россией и ответственности за гибель российских военнослужащих и мирных граждан Донбасса.

В дальнейшем MetaConstellation был дополнительно реализован в комплексе по увеличению возможностей ударных беспилотников Skykit. Он представляет собой большой «чемодан», оснащенный аккумуляторами, двумя встроенными мониторами, ноутбуком, дроном Quadcopter, антенной, камерой Trailcam Nano. Программное обеспечение Meta-Constellation позволяет подключаться к одному из 40 коммерческих спутников, ежедневно пролетающих над Украиной, собирать и анализировать обработанные искусственным интеллектом данные. Это помогает отслеживать российские войска на территории Украины.

Palantir официально представила Skykit в январе 2023 года на выставке Consumer Electronics Show. По данным военных Telegram-каналов, комплексы Skykit попали в зону конфликта, как минимум, в феврале 2023-го. Официально это признали в сентябре 2023 года, когда в Объединённом центре компетенции ВВС НАТО в немецком Калькаре состоялась встреча представителей альянса и военных структур киевского режима. Возглавлявший украинскую делегацию подполковник Ярослав Гончар сообщил о том, что ВСУ активно используют предоставленную им Palantir технологию Skykit, позволяющую усовершенствовать процесс получения данных с БПЛА в режиме реального времени.

Комплекс Skykit на Украине

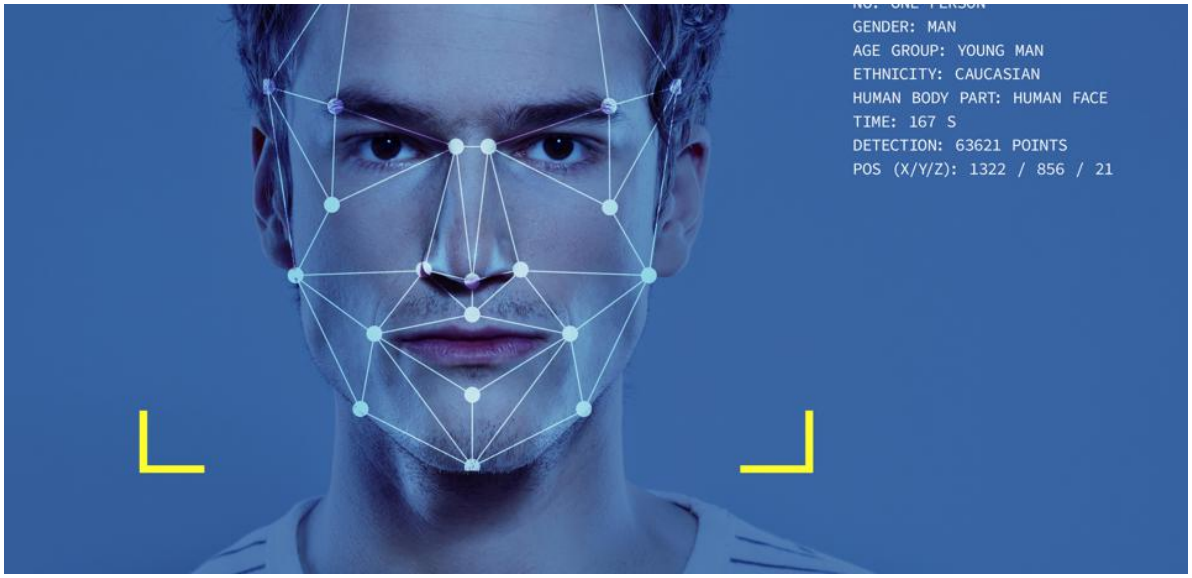
Другим направлением использования технологий американской компании в боевых действиях на Украине должен был стать совместный проект Palantir и небезызвестной Open AI под названием Maven. По замыслу разработчиков, система предназначалась для автоматического обнаружения целей и наведения на них роя автономных дронов-камикадзе при минимальном участии человека-оператора. Известно, что в 2023 году программа начала тестироваться на Украине. Но судя по всему, успехов не достигла и заглохла. Ни одна из сторон конфликта не подтверждала применение таких дронов на поле боя.

Изначально в Palantir утверждали, что работают на Украине фактически бесплатно. Имелось в виду, конечно, отсутствие чистой прибыли, потому что компания всё равно получала своё – через политическую поддержку от американского руководства, новые возможности для рекламы и рост капитализации. Тем не менее, отчётность, опубликованная в конце 2022 года, показала, что про денежный вопрос никто не забывал. Согласно документам, Palantir и её дочерние структуры только за первые месяцы работы на Украине получили более $500 млн. Скорее всего, большая часть из этих денег была направлена на устранение выявленных в ходе испытаний дефектов и закупку дополнительного оборудования или запасных частей. Украинские солдаты неоднократно жаловались, что поставляемая западная помощь не адаптирована под реалии современных боевых действий и плохо функционирует в наших погодных и географических условиях. Более того, склады с западными «товарами» регулярно становятся целью российских ракет и беспилотников. Я не исключаю, что большой объем

поставленного оборудования мог быть уничтожен в результате российских ударов, и выделенные средства также включают в себя пункт о поставках новых образцов, взамен утраченных.

В апреле 2024 года украинские СМИ сообщили о том, что СБУ использует ещё одну разработку Palantir, также основанную на ИИ, для анализа массивов данных с целью поиска «предателей». В этом случае уже речь идет о работе с персональными данными украинских граждан. Как и в скандальных эпизодах в Великобритании и других странах такая деятельность явно связана с нарушением базовых гражданских прав и свобод. Но, к сожалению, здесь у Palantir руки развязаны полностью: никто не будет поднимать бучу и бороться за права украинцев. К тому же этот инструмент может активно применяться для поиска уклонистов для их последующей отправки на фронт.

Еще один «партнер» киевского режима – американская **Clearview AI**, Inc. Она специализируется на производстве программного обеспечения для распознавания лиц. История компании началась в 2017, но резкий рост наметился спустя два года, когда её продукцией начали активно пользоваться сотрудники правоохранительных органов США. В распоряжении компании сейчас находятся около 30 млрд изображений пользователей, полученных в основном из социальных сетей - без разрешения их владельцев. В итоге, Clearview стало инструментом спецслужб. К началу СВО это уже был мощный инструмент, применяемый Вашингтоном не только на своей, но и на чужой территории.



Программное обеспечение Clearview

Бэкграунд Clearview также крайне противоречив. Оказалось, что компания создавала базы данных из личной информации и фотографий подданных Нидерландов. В чьих интересах и для чего это делалось, долгое время оставалось загадкой. У нидерландского руководства были вполне резонные основания для того, чтобы подозревать Clearview в незаконном использовании персональных данных.

Изначально в компании утверждали, что заказчиком были спецслужбы стран Евросоюза. В королевстве возмутились деятельностью компании и в результате судебного разбирательства на компанию наложили штраф в размере 30,5 млн евро за нарушение законодательства в сфере защиты персональных данных. В конце концов, представители Clearview признали, что данные о жителях Нидерландов собирали в интересах американских разведывательных служб, а не европейских.

Аналогичные преступления Clearview были выявлены и в других странах Европы и в Австралии. Компанию не раз штрафовали на

миллионы долларов за нарушение неприкосновенности частной жизни.

В 2020 году хакеры смогли получить доступ к внутренней информации Clearview, из которой прямо следовало, что компания незаконно собирала данные миллионов пользователей крупнейших соцсетей, включая Facebook, Instagram и Twitter, а также других ресурсов, в том числе сервисов Google. Причем дело не ограничивалось только фотографиями. Например, приложение Clearview для Android собирало информацию о местоположении мобильного устройства, данные голосового поиска и даже штрих-коды с водительских прав. Скандал привел к тому, что приложение было удалено из App Store, а против самой компании начали подавать иски.

Любопытно, что многие американские СМИ, в частности, New York Times, которая выпустила целое расследование по этой теме, обвиняли Clearview в продаже получаемой информации правоохранительным органам. По мнению журналистов, это грубо нарушало принцип свободы личности. Однако в реальности ситуация была намного хуже. Как показал эксперимент, проведенный специалистами фирмы SpiderSilk, специализирующейся в области кибербезопасности, исходный код приложения Clearview содержал достаточное количество ошибок, чтобы любой умелый хакер мог получить доступ к собираемым компанией данным и затем использовать их в своих целях.

Кроме того, критики считают, что использование программ Clearview полицией фактически делает любого гражданина «подозреваемым во всех преступлениях сразу». Американский союз гражданских свобод ранее уже обращался в суд штата Иллинойс, обвиняя компанию в нарушении законодательства.

После этого большинству американских коммерческих компаний запрещено сотрудничать с Clearview.

Украинский конфликт, как и для Palantir, стал шансом отмыть репутацию фирмы поправить пошатнувшееся финансовое положение. Уже в апреле 2022 года Washington Post опубликовал материал, в котором рассказывалось о вовлеченности Clearview в конфликт. По данным журналистов, боевики ВСУ тайно передавали представителям компании фотографии убитых российских солдат, чтобы можно было идентифицировать как их самих, так и их родственников. Полученные таким образом данные киевский режим использовал для поиска контактных данных родных погибших российских военнослужащих. Затем нацисты обзванивали родственников, в издевательской форме сообщали о гибели их близкого, доводили до истерики. Зачастую, новость о смерти сопровождалась отправленными фото или видеофайлами, на которых солдаты ВСУ глумились над телом убитого.

Украинский военнослужащий звонит матери погибшего солдата ВС РФ

Примечательно, что после публикации в WP было много возмущения даже в самих западных странах. Комментируя этот процесс, авторы материала назвали такое использование технологии Clearview «ужасным». А в крупной британской НКО Privacy International даже призвали руководство компании немедленно прекратить их деятельность на Украине, заявив о том, что её потенциальные последствия нельзя терпеть ни при каких условиях.

Однако в руководстве Clearview общественным осуждением

нисколько не смутились. Основатель и генеральный директор компании Хоан Тон-Тхат даже не стал комментировать обвинения в свой адрес. Вместо этого он похвастал, что благодаря разработке новых технологий его компании удалось успешно просканировать российскую социальную сеть «Вконтакте».

В апреле 2023 года Тон-Тхат посетил Киев, где встретился с главой ГУР МО Украины Кириллом Будановым и получил от него благодарность «за помощь Минобороны и ВСУ».

Кирилл Буданов и Хоан Тон-Тхат

Американские компании в тех случаях, когда это нужно руководству США, спокойно нарушают закон и в самих Штатах, и в странах Европы. Очевидно, что на подконтрольных киевскому режиму территориях, где само понятие «закон» давно превратилось в фарс, им дан полный карт-бланш на любую, в том числе откровенно криминальную деятельность.

Алекс Карп и Тон-Тхат фактически такие же наемники, как и боевики из «Интернационального легиона», которые приехали убивать за деньги. Для них война – это бизнес. Закончится здесь, они будут лоббировать начало нового конфликта.

Кроме того, необходимо подчеркнуть, что переданное ВСУ оборудование и технологии активно применяются и против "партнеров" Киева. А по мере завершения конфликта количество пострадавших от рук украинцев американцев и европейцев будет только возрастать. Если не верите, то спросите об этом поляков, которые уже перевели миллионы евро украинским мошенникам.