ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«ГЛАВНЫЙ РАДИОЧАСТОТНЫЙ ЦЕНТР»
(ФГУП «ГРЧЦ»)

НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

РАСШИРЕННАЯ АНАЛИТИЧЕСКАЯ СПРАВКА
Технологические инструменты мягкой силы США

Москва
2026

ОГЛАВЛЕНИЕ

[1] Признана экстремистской и запрещена на территории РФ.

ВВЕДЕНИЕ

Мягкая сила (soft power) – это способность страны оказывать влияние на другие государства и общества без применения военной и другой «жесткой» силы. Концепция мягкой силы была введена американским политологом Джозефом Наем в 1990 году.

Мягкая сила США включает в себя широкий спектр компонентов, к числу которых относятся:

1. Культурное влияние:

– американская массовая культура;

– доминирование американской киноиндустрии и музыкальной индустрии;

– американская культура потребления, образ жизни, система ценностей.

2. Информационно-коммуникационное доминирование:

– глобальные медиа, формирующие мировую информационную повестку;

– вещание региональных проамериканских СМИ;

– контроль над основными платформами распространения информации, алгоритмами и политикой социальных сетей и других социальных медиа;

– экосистема американских и проамериканских каналов в социальных сетях, блогеров и других инфлюенсеров;

– инфраструктура информационно-коммуникационных суррогатов (боты, аккаунты, каналы, генераторы информации);

– влияние на мировую цифровую инфраструктуру, интернет-стандарты и т. п.

3. Политическое влияние:

– продвижение «либеральных» и «демократических» ценностей;

– ведущая роль в международных и глобальных организациях и институтах;

– использование публичной дипломатии, стратегической коммуникации и др.;

– поддержка проамериканских режимов местных политических оппозиций.

4. Экономическое влияние:

– сохранение лидирующего положения американского доллара;

– финансовая поддержка США, американских фондов и проамериканских ТНК;

– глобальное влияние американских компаний и проамериканских ТНК;

– технологическое доминирование;

– влияние на рынки и распределение мировых ресурсов.

5. Научно-образовательное влияние:

– привлечение студентов, ученых из других стран, программы обмена;

– система грантов и финансирования исследований;

– влияние через международные научные организации, академическую систему.

6. Неправительственные, некоммерческие организации и агентурная сеть:

– деятельность американских и проамериканских НПО и НКО;

– система грантов и финансирования НПО и НКО других стран;

– деятельность агентурной, посреднической и марионеточной сети на местах.

7. Другие инструменты мягкой силы:

С приходом новой администрации Дональда Трампа США приостановили финансирование большинства крупных организаций, которые годы и десятилетия считались проекцией мягкой силы Штатов, таких как USAID, NED, GEC DOS и др.

Цель реформы институтов мягкой силы США – заменить устаревшие коррумпированные структуры на более рентабельные и эффективные инструменты на основе искусственного интеллекта.

Таким образом, **технологические инструменты мягкой силы** становятся следующим поколением в методологии американского информационного влияния. К технологическим инструментам мягкой силы США в первую очередь относятся современные цифровые, информационно-коммуникационные и ИИ-системы, сервисы, технологии и инструменты, способствующие американскому доминированию и влиянию в мировом информационном и киберпространстве.

Управление перспективных исследовательских проектов Министерства обороны США (DARPA), Агентство передовых исследований в сфере разведки (IARPA), а также инвестиционные фирмы – посредники американских специальных служб, такие как In-Q-Tel, активно спонсируют разработку новых технологий на основе анализа больших данных, моделирования социальных процессов и предиктивной аналитики для использования в военных, разведывательных и внешнеполитических целях.

Большая часть таких технологических инструментов мягкой силы оказывается в руках Киберкомандования США (US CYBERCOM), сил специальных операций (PSYOP) и американских специальных служб. Данные инструменты используются для организации и проведения киберразведки и кибершпионажа, информационно-психологических операций и кампаний, оказания долгосрочного информационно-психологического влияния на население других стран.

Кроме того, большая часть американских цифровых гигантов, платформ и социальных медиа активно сотрудничают с правительством, Министерством обороны и специальными службами США, также являясь технологическими инструментами мягкой силы США, обеспечивая превосходство Соединенных Штатов в мировом информационном и киберпространстве.

ПРОГРАММЫ DARPA

Некоторые программы **Управления перспективных исследовательских проектов Министерства обороны США** (далее – DARPA), способствовавшие развитию мягкой силы США через технологическое лидерство, информация о которых есть в открытых источниках.

Программа SMISC[1] (Social Media in Strategic Communication).

Старт программы – 2011 год.

Основная цель – разработка автоматизированных и полуавтоматических инструментов для анализа социальных сетей.

Задачи программы включали:

– выявление, классификацию, измерение и отслеживание формирования, развития и распространения идей, концепций, мемов, преднамеренной дезинформации и противоправной пропаганды в социальных сетях;

– понимание структуры кампаний убеждения и операций влияния в социальных сетях и сообществах;

– выявление участников, их намерений и оценка эффективности кампаний убеждения;

– противодействие выявленным операциям влияния противников.

Программа SocialSim[2] (Computational Simulation of Online Social Behavior).[3]

Старт программы – 2017 год.

Основная цель – прогнозирование динамики онлайн-поведения, включая распространение дезинформации, реакции на кризисы и формирование общественного мнения.

Задачи программы включали:

– разработку высокоточных вычислительных симуляторов распространения и эволюции информации в социальных сетях;

– создание технологий, способных точно моделировать распространение онлайн-информации среди целевых групп населения;

– разработку эффективных и надежных методов предоставления данных для поддержки разработки, тестирования и оценки моделирования.

Программа Ground Truth[4]**.**

Старт программы – 2017 год.

Основная цель [5] – разработка инструментов для моделирования и прогнозирования социальных реакций на информационные кампании, включая PSYOP и операции влияния.

Задачи программы включали:

---

[1] idstch.com/technology/ict/darpa-using-mind-control-techniques-manipulate-social-media/

[2] academia.edu/121337437/The_DARPA_SocialSim_Challenge_Massive_Multi_Agent_Simulations_of_the_Github_Ecosystem

[3] idstch.com/technology/ict/darpa-socialsim-developing-effective-information-warfare-analysis-tools-for-social-media/

[4] darpa.mil/program/ground-truth

[5] nap.nationalacademies.org/read/25271/chapter/12

– создание симуляций и моделей социальных систем с использованием ИИ для проверки гипотез о поведении и взаимодействиях в социальных сетях;

– создание «цифровых двойников» социальных сред для анализа влияния информации и прогнозирования последствий;

– изучение причин сложного социального поведения;

– проверку последствий политических решений.

Программа NGS2[1] (Next Generation Social Science).[2]

Старт программы – 2019 год.

Основная цель – создание и оценка новых методов и инструментов для вычисления и обоснования моделей социального поведения человека.

Задачи программы:

– выявление механизмов формирования «коллективного я»;

– изучение факторов, влияющих на групповое поведение через теорию игр и эволюционное моделирование;

– изучение социальных динамик и темпоральных изменений в социальных нормах и коллективной идентичности;

– разработка предсказательных моделей поведения групп и индивидов.

Программа ASIST[3] (Artificial Social Intelligence for Successful Teams).[4]

Старт программы – 2019 год.

Основная цель – разработка теории и систем искусственного интеллекта, которые смогут понимать цели и убеждения людей, предсказывать их потребности и предлагать контекстно ориентированные вмешательства.

Задачи программы:

– разработка машинной теории разума; ИИ-агенты должны выводить ментальные состояния людей на основе наблюдаемых действий и контекста;

– создание общих ментальных моделей для ИИ-агентов для согласования их понимания окружающей среды, оборудования и стратегий людьми;

– создание настраиваемой среды открытого мира со стандартизированными интерфейсами для оценки ИИ-агентов.

Программа INCAS[5] (INfluence Campaign Awareness and Sensemaking).[6]

Старт программы – 2020 год.

Основная цель – создание инструментов для обнаружения и анализа кампаний геополитического влияния.

Задачи программы:

---

[1] nap.nationalacademies.org/read/25271/chapter/12

[2] idstch.com/technology/ict/darpa-next-generation-social-science-program-seek-new-models-theories-tools-predictive-science-social-phenomena/

[3] darpa.mil/program/artificial-social-intelligence-for-successful-teams

[4] idstch.com/technology/ict/artificial-social-intelligence-for-successful-teams-asist-pioneering-human-machine-collaboration/

[5] darpa.mil/program/influence-campaign-awareness-and-sensemaking

[6] sociable.co/social-media/darpa-to-exploit-social-media-messaging-blog-data-to-track-geopolitical-influence-campaigns/

– автоматическое обнаружение признаков влияния в многоязычных онлайн-сообщениях;

– анализ психографических атрибутов, таких как мировоззрение, мораль и ценности;

– анализ текста и онлайн-поведения для извлечения психографических атрибутов и их соотнесения с показателями влияния в сообщениях, на которые реагирует определенный сегмент населения;

– моделирование динамики кампаний для объяснения и прогнозирования реакций населения.

Программа Habitus.[1]

Старт программы – 2020 год.

Основная цель[2] – разработка ИИ для анализа социальных и культурных факторов, влияющих на восприятие информации в цифровых средах.

Задачи программы:

– моделирование региональных культурных норм и ценностей для понимания поведения местных социальных групп;

– разработка AI-механизмов взаимодействия с жителями различных регионов;

– разработка адаптивных ИИ-инструментов для прогнозирования реакций на информационные кампании в различных регионах;

– разработка инструментов для прогнозирования и управления информационными потоками в условиях геополитических конфликтов и операций влияния.

Программа SemaFor[3] (Semantic Forensics).[4]

Старт программы – 2021 год.

Основная цель – автоматизация поиска и экспертизы содержания мультимедийных материалов (текстов, аудио, изображений, видео).

Задачи программы:

– определение намерений и смысла манипуляций на семантическом уровне;

– создание интеграционных мультимодальных ИИ-моделей;

– создание инструментов локализации манипуляций внутри медиа;

– защита от крупномасштабных дезинформационных атак в режиме реального времени.

Программа CCU[5] (Computational Cultural Understanding).[6]

Старт программы – 2021 год.

Основная цель – компьютерное изучение и технологическое применение знаний об эмоциональных, социальных и культурных нормах общения в различных странах, языках и социальных группах.

---

[1] darpa.mil/work-with-us/information-innovation-office
[2] sociable.co/technology/local-mentality-darpa-program-has-non-military-potential-for-learning-about-different-cultures/
[3] darpa.mil/program/semantic-forensics
[4] insights.sei.cmu.edu/library/darpas-sematic-forensics-semafor-research-program/
[5] darpa.mil/program/computational-cultural-understanding
[6] idstch.com/technology/ict/darpa-ccu-developing-ai-enabled-automated-cultural-interpreters-and-dialogue-assistants/

Задачи программы:

– автоматизированное распознавание и изучение социокультурных норм, эмоционального реагирования и особенностей коммуникации в различных культурах и сообществах;

– разработка систем для повышения успеха в межкультурном взаимодействии;

– сбор баз данных различных культур общения для обучения будущих систем и тестирования коммуникации с их использованием.

Программа Civil Sanctuary.[1]

Старт программы – 2021 год.

Основная цель – разработка многоязычных ИИ-модераторов для социальных медиа, которые будут минимизировать «деструктивные идеи» и поощрять «полезные поведенческие нормы».

Задачи программы:

– расширение возможностей модерации существующих платформ;

– обучение искусственных агентов лучшим практикам онлайн-посредничества на основе наблюдений за людьми;

– обеспечение стабильной информационной среды во время гуманитарных операций и кризисов.

Программа MIP[2] (Modeling Influence Pathways).[3]

Старт программы – 2022 год.

Основная цель – разработка инструментов моделирования путей распространения информации с нишевых платформ в мейнстрим.

Задачи программы:

– структурный и временной анализ информационных потоков;

– выявление взаимосвязей между различными каналами распространения информации для понимания их роли в операциях влияния;

– создание карт информационных потоков;

– выявление характерных паттернов и закономерностей путей влияния;

– дополнение существующих возможностей обнаружения дезинформации.

[1] sociable.co/technology/darpa-ai-moderate-social-media-groups-destructive-ideas-humanitarian-efforts/
[2] darpa.mil/news-events/2022-05-04a
[3] strangesounds.org/2022/05/darpa-wants-to-model-how-disinformation-flows-from-fringe-to-mainstream-platforms.html

PALANTIR

Palantir Technologies Inc. [1] – американская компания, разработчик программного обеспечения анализа больших данных, моделирования, предиктивной аналитики, систем поддержки принятия решений и автоматизации процессов на основе ИИ.

Инструменты Palantir применяются в сферах обороны, разведки, финансов, государственного управления, медиа, здравоохранения, бизнеса и др.

Компания основана Питером Тилем, Стивеном Коэном, Джо Лонсдейлом и Алексом Карпом в 2003 году. Председатель совета директоров – Питер Тиль, генеральный директор – Алекс Карп.

Штаб-квартира компании расположена в Денвере (штат Колорадо), представительства открыты в 19 странах. Штат компании – около 4 тыс. сотрудников.

По состоянию на июнь 2025 года капитализация компании составляла около 300 млрд долларов, за полгода после прихода администрации Д. Трампа она выросла примерно в шесть раз.

Gotham – разработка компании Palantir в области обороны и разведки. Она является развитием многолетней работы Palantir в разведывательном сообществе США. Изначальное наименование продукта – Government – отражало секторальную специфику.

Основная концепция продукта – визуализация больших массивов данных из разнородных источников, позволяющая пользователям без технической подготовки находить взаимосвязи между объектами, обнаруживать совпадения между объектами и событиями вокруг них, выявлять аномальные объекты, анализировать ситуацию и принимать наилучшие варианты реагирования в рамках быстро изменяющихся условий (например, войны нового типа или стихийных бедствий) – фактический Data Mining с упором на интерактивный визуальный анализ в духе концепции «усиления интеллекта».

В качестве источников программное обеспечение Palantir использует как традиционные базы данных и другие структурированные источники, так и неструктурированные источники: тексты, аудио, видео. При этом заявляется, что для непосредственного использования продуктов организациям-заказчикам не требуется персонал с инженерными или программистскими навыками, так как вся работа ведется в интуитивном графическом пользовательском интерфейсе, а запросы к источникам формулируются на естественном языке.

Центральный механизм хранения в Gotham использует технику онтологий, средствами которых разнородные данные из множества источников оснащаются смысловой информацией и унифицируются для совместного анализа. Онтологии в продуктах Palantir могут быть одного из трех типов:

– сущности – субъекты или объекты реального мира;

[1] palantir.com/palantir-is-not-a-data-company/

– события – действия над сущностями, происходящие в определенный момент времени и в определенной точке пространства;

– документы – подтверждения сведений о реальном мире, сведенные в унифицированный формат (используется HTML).

Средства семантического поиска в платформе используют возможности составления сложных запросов к онтологиям, в частности, поддерживается поиск по близости значения, есть также средства фонетического поиска. Установленные пользователями-аналитиками факты и взаимосвязи также хранятся в семантической форме и участвуют в последующем анализе. Платформой поддерживается подключение генетических алгоритмов, специализированным образом разрабатываемых для тех или иных сфер деятельности. Также составной частью платформы является подсистема групповой работы пользователей, позволяющая аналитикам обмениваться сообщениями и результатами анализа.

Платформа Palantir Gotham открыта и может быть расширена в соответствии с нуждами пользователей, адаптирована практически к любому программному и аппаратному обеспечению. Под открытостью понимается наличие открытого интерфейса программирования приложений (Public API) к любой функции, расширяемая архитектура, динамические онтологии, которые могут быть адаптированы к предметной области, возможность использования дополнительных способов интеграции данных, открытый экспорт данных и API к данным без каких-либо ограничений со стороны производителя.

По состоянию на 2013 год клиентами компании Palantir были: Министерство внутренней безопасности США, АНБ, ФБР, Корпус морской пехоты, ВВС, Командование специальных операций, Военная академия, Объединенная организация по уничтожению самодельных взрывных устройств и союзники США. Кроме того, по данным TechCrunch, «шпионские агентства США также использовали Palantir для соединения баз данных разных ведомств»: «До этого большинство баз данных, используемых ЦРУ и ФБР, были разрозненными, что вынуждало пользователей искать в каждой базе по отдельности. Теперь все связано вместе с помощью Palantir»[1].

В 2011 году появилась информация, что Palantir причастна к программе противодействия проекту WikiLeaks [2] . Активисты хакерской организации Anonymous выяснили, что специалисты Palantir предлагали властям США использовать кибератаки и дезинформацию для противодействия неугодным журналистам.

Разработки Palantir активно используются вблизи линии фронта на украинском ТВД[3]. Они применяются для сокращения «цепочки поражения»[4] в

[1] techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/
[2] thetechherald.com/articles/Data-intelligence-firms-proposed-a-systematic-attack-against-WikiLeaks/12751/
[3] time.com/6691662/ai-ukraine-war-palantir/
[4] Военная концепция, определяющая структуру атаки. Она состоит из идентификации цели, отправки сил и средств к цели, начала атаки на цель и уничтожения цели.

военных действиях. Согласно отчету The Times от декабря 2022 года, искусственный интеллект Palantir позволил Украине повысить точность, скорость и смертоносность артиллерийских ударов.[1]

Palantir также предоставляет услуги разведки и наблюдения Армии обороны Израиля (ЦАХАЛ). В январе 2024 года Palantir договорилась о стратегическом партнерстве с ЦАХАЛ, в рамках которого она будет предоставлять ЦАХАЛ услуги для помощи в выполнении «военных миссий»[2].

Применение Palantir как инструмента мягкой силы

1. Анализ информационных потоков.

Платформы Palantir интегрируют данные из множества источников, включая социальные сети, публичные записи и закрытые базы данных, для анализа информационных потоков. Они позволяют выявлять тренды, ключевых акторов и источники информации.

Palantir использует данные из социальных сетей и с низкоорбитальных спутников для анализа информации, что позволяет объединять открытые источники (OSINT) с агентурными сводками[3].

Примеры применения. Palantir использовалась для мониторинга социальных сетей в интересах правоохранительных органов и разведки. Например, в рамках контрактов с DHS (2024–2025)[4].

2. Анализ социальных сетей и цифровых следов.

Патентная технология (2023). Palantir разработал системы для атрибуции данных к субъектам через анализ разрозненных наборов данных из соцсетей и других цифровых источников. Метод включает:

– создание «траекторий» поведения на основе записей, связанных с субъектом (например, история действий в аккаунтах);

– идентификацию связей между аккаунтами, устройствами и IP-адресами для установления цифровых профилей.

Примеры применения. Использование в финансовых расследованиях для выявления мошеннических схем через корреляцию трансакций с активностью в соцсетях[5].

3. Операции влияния, информационные кампании и PSYOP.

Платформы Palantir используется разведсообществом США для интеграции данных из соцсетей, финансовых отчетов, перехвата коммуникаций и геоданных[6].

Palantir AIP (Artificial Intelligence Platform) поддерживает анализ целевых аудиторий, моделирование сценариев и таргетинг. Palantir Gotham используется для обработки разведданных, включая социальные и культурные факторы.

---

[1] thetimes.co.uk/article/ukraine-is-outflanking-russia-with-ammunition-from-big-tech-lxp6sv3qz
[2] bloomberg.com/news/articles/2024-01-12/palantir-israel-agree-to-strategic-partnership-for-battle-tech
[3] d-russia.ru/tag/palantir
[4] nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html
[5] supplychaintoday.com/palantir-technologies-cheat-sheet/
[6] techgolly.com/palantir-and-the-role-of-big-data-in-government-surveillance

Технологии Palantir поддерживают разведывательные и военные операции США, где информационное влияние играет ключевую роль. Например, Gotham используется в военных кампаниях для анализа больших интернет-данных[1].

В прошлом компания сотрудничала с Cambridge Analytica, что также указывает на потенциал Palantir в таргетированной пропаганде и манипулятивных практиках[2].

3. Анализ культурных особенностей социальных групп.

Инструменты Palantir могут анализировать демографические и социокультурные данные, выявляя нормы и ценности групп. Это полезно для адаптации стратегий к региональным контекстам.

Примеры применения. Palantir поддерживает анализ культурных контекстов в военных операциях за рубежом, где понимание местных обычаев критично[3]. То же самое Palantir может осуществлять для применения «мягких» стратегий.

4. Изучение и манипуляция поведением.

Платформы Palantir используют психографику и поведенческий анализ, интегрируя данные из социальных сетей, геолокации, финансовых трансакций и других источников для создания детализированных профилей индивидов и групп. Это позволяет прогнозировать поведение и выявлять паттерны.

Примеры применения. В коммерческом секторе Foundry применяется для прогнозирования потребительского поведения. Например, Morgan Stanley использует Palantir для анализа рыночных трендов и клиентских предпочтений[4].

В государственных проектах Palantir сотрудничала с ICE (2014–2025), отслеживая мигрантов через данные соцсетей, геолокации и транзакций, усиление контроля за перемещениями[5].

Программа Metropolis (ранее Palantir Finance) использовалась JPMorgan для мониторинга активности сотрудников, включая анализ переписки и поведения[6].

Подобные практики вызывают обеспокоенность из-за нарушения приватности и потенциального профилирования. Правозащитные организации, такие как Amnesty International, критикуют Palantir за недостаточную прозрачность в использовании данных[7].

5. Социальное моделирование и прогнозирование.

Платформы Palantir, особенно Foundry и AIP, используют предиктивную аналитику и машинное обучение для прогнозирования социальных и экономических трендов. Они обрабатывают исторические данные, текущие события и социальные сигналы, чтобы предсказывать реакции общества или развитие кризисов. Palantir Foundry и AIP создают цифровые модели (онтологии)

---

[1] palantir.com/offerings/intelligence/
[2] en.wikipedia.org/wiki/PalantirTechnologies
[3] graniteshares.com/institutional/us/en-us/research/what-does-palantir-technologies-do
[4] palantir.com/platforms/foundry/
[55] nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html
[6] en.wikipedia.org/wiki/Palantir_Technologies
[7] amnesty.org.nz/palantir-technologies-contracts-raise-human-rights-concerns-nyse-direct-listing/

для симуляции социальных систем, анализа взаимодействий и прогнозирования трендов. AIP использует большие языковые модели для моделирования сложных сценариев, включая общественные реакции.

Примеры применения. Palantir Foundry применяется для прогнозирования кризисов, таких как сбои в цепочках поставок или гуманитарные ситуации. Например, в 2024 году Palantir использовалась для моделирования логистики в кризисных зонах1.

Palantir помогает прогнозировать сбои в цепочках поставок или рыночные изменения. Например, в 2024 году Palantir работала с компаниями в сфере здравоохранения для прогнозирования спроса на медицинские ресурсы во время вспышек заболеваний2.

В военных и разведывательных контекстах Palantir поддерживает прогнозирование социальных волнений или реакции населения на военные действия. Например, их технологии использовались для анализа данных в Афганистане для предсказания активности повстанцев.[3]

6. Киберрасследования и выслеживание.

Gotham интегрирует данные с камер наблюдения, из социальных сетей, финансовых транзакций и других источников для создания профилей и отслеживания активности. Это помогает выявлять угрозы и координировать операции.

Примеры применения. В США Palantir сотрудничала с полицией Нью-Йорка и Лос-Анджелеса для анализа данных в реальном времени, включая социальные сети, для предотвращения преступлений[4].

В международном контексте Palantir поддерживает контртеррористические операции, анализируя данные для выявления сетей экстремистов. Например, в 2023 году сообщалось о применении Gotham для анализа данных в борьбе с ISIS[5].

7. Роль в кризисном управлении.

Платформа Foundry позволяет моделировать кризисные сценарии, анализировать данные в реальном времени и координировать действия между различными агентствами и организациями. Она интегрирует данные из множества источников для быстрого принятия решений.

Примеры применения. Во время пандемии COVID-19 (2020–2022) Palantir сотрудничала с CDC и NHS для анализа данных о распространении вируса, распределения вакцин и управления медицинскими ресурсами[6].

В 2024 году Palantir использовалась для управления гуманитарными кризисами, включая анализ данных о перемещении беженцев и прогнозирование

---

[1] palantir.com/impact/world-food-programme/
[2] palantir.com/uk/healthcare/
[3] wired.com/story/palantirs-gods-eye-view-of-afghanistan/
[4] forbes.com/sites/michaelposner/2019/09/12/what-companies-can-learn-from-palantir/
[5] graniteshares.com/institutional/us/en-us/research/what-does-palantir-technologies-do
[6] nytimes.com/interactive/2020/10/21/magazine/palantir-alex-karp.html?ysclid=mc7pzcm92k679859992

потребностей в гуманитарной помощи в зонах конфликтов, таких как Украина и Ближний Восток[1].

8. Интеграция с другими технологиями и платформами.

Palantir Apollo обеспечивает развертывание и управление аналитическими приложениями, что позволяет интегрировать их технологии с другими системами, включая облачные платформы и ИИ-инструменты.

Примеры применения. В 2025 году Palantir расширила интеграцию с AWS и Microsoft Azure для обработки данных в реальном времени, что усилило их возможности в анализе социальных сетей и информационных потоков[2].

AIP позволяет создавать ИИ-агенты, которые могут взаимодействовать с данными из соцсетей или моделировать сценарии для военных и коммерческих клиентов[3].

Потенциал. Интеграция с внешними платформами делает Palantir универсальным инструментом для сложных задач, таких как мониторинг дезинформации в реальном времени или моделирование общественных реакций.

9. Будущие направления.

В 2025 году Palantir продолжает развивать свою платформу AIP (Artificial Intelligence Platform), усиливая интеграцию больших языковых моделей и автоматизированного анализа для задач, связанных с прогнозированием социальных и политических событий. Также наблюдается фокус на кибербезопасность, включая мониторинг информационных угроз и дезинформации[4].

Потенциал. Palantir может стать ключевым игроком в создании систем для прогнозирования глобальных социальных и политических трендов, особенно в области борьбы с дезинформацией и кибератаками. Расширение сотрудничества с облачными платформами, такими как AWS и Microsoft Azure, усиливает их возможности для обработки данных в реальном времени, что может быть использовано для анализа социальных сетей и моделирования общественных реакций.

[1] wfp.org/news/palantir-and-wfp-partner-help-transform-global-humanitarian-delivery
[2] palantir.com/partnerships/aws/
[3] palantir.com/platforms/aip/
[4] reuters.com/business/palantir-raises-annual-revenue-forecast-booming-ai-demand-2025-05-05/

ДРУГИЕ КОМПАНИИ И ТЕХНОЛОГИЧЕСКИЕ ИНСТРУМЕНТЫ МЯГКОЙ СИЛЫ США

Meta Platforms[1]

Meta Platforms, Inc.[2] – американская компания, основанная в 2004 году как Facebook, со штаб-квартирой в Менло-Парк, Калифорния. Владеет социальными сетями (Facebook, Instagram, WhatsApp) и развивает технологии виртуальной и дополненной реальности (Quest, Ray-Ban Stories). Фокусируется на метавселенной и цифровой рекламе.

Продукты и инструменты: Facebook, Instagram, WhatsApp, Meta AI, Facebook Ads, Audience Insights и алгоритмы рекомендаций для контента.

Области применения в социальном управлении и влиянии: таргетированная пропаганда, манипуляция рекомендательными системами, анализ цифровых следов, анализ психографики и поведения, использование ботов.

Описание и примеры:

– Таргетированная пропаганда: Facebook Ads позволяет нацеливать рекламу на основе детальных данных пользователей. Пример: использование Cambridge Analytica данных Facebook для таргетинга в кампании 2016 года в США[3].

– Манипуляция рекомендательными системами: алгоритмы Facebook и Instagram продвигают контент для повышения вовлеченности. Пример: продвижение дезинформации о выборах 2020 года на Facebook, усилившее поляризацию[4].

– Анализ цифровых следов: Audience Insights собирает данные о поведении пользователей. Пример: сотрудничество с АНБ в рамках PRISM для анализа данных пользователей Facebook.[5]

– Анализ психографики и поведения: Meta AI создает профили на основе активности пользователей. Пример: использование данных Meta AI для анализа предпочтений избирателей в 2018 году в Бразилии6.

– Использование ботов: платформы Meta уязвимы для ботов, распространяющих дезинформацию, и используются США и их противниками в соответствующих целях[7].

---

[1] Признана экстремистской и запрещенна на территории РФ.
[2] meta.com
[3] nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html
[4] washingtonpost.com/technology/2020/11/01/facebook-election-misinformation/
[5] theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[6] blogs.lse.ac.uk/polis/2018/10/27/2018-brazil-elections-the-power-of-social-media-and-the-threat-to-journalism/
[7] currenttime.tv/a/video-kak-rabotayut-boty-v-sotssetyah/30200604.html

Google (Alphabet Inc.)

Alphabet Inc.[1] – американская холдинговая компания, основанная в 2015 году как реорганизация Google, со штаб-квартирой в Маунтин-Вью, Калифорния. Google – основное подразделение, предоставляющее поисковые, облачные (Google Cloud) и рекламные услуги, а также продукты вроде Android, YouTube и Pixel. Alphabet инвестирует в ИИ, автономный транспорт (Waymo) и другие инновации. Публичная компания (NASDAQ: GOOGL).

Продукты и инструменты: Google Cloud Platform (GCP), Google Analytics, TensorFlow, YouTube recommendation algorithms, Google Ads и инструменты анализа данных (BigQuery).

Области применения в социальном управлении и влиянии: таргетированная пропаганда, манипуляция рекомендательными системами, анализ цифровых следов, массовая слежка.

Описание и примеры:

– Таргетированная пропаганда: Google Ads позволяет нацеливать рекламу на основе пользовательских данных, включая политические предпочтения. Пример: использование Google Ads в кампании 2016 года для продвижения политической дезинформации в США[2].

– Манипуляция рекомендательными системами: алгоритмы YouTube продвигают контент, увеличивающий вовлеченность, что может усиливать поляризующий контент. Пример: продвижение радикальных видео во время выборов[3].

– Анализ цифровых следов: Google Analytics и BigQuery собирают данные о поведении пользователей. Пример: сотрудничество с АНБ в рамках PRISM для предоставления данных о поисковых запросах и активности пользователей[4].

– Массовая слежка: GCP используется для обработки больших объемов данных для разведки. Пример: контракт Google с Пентагоном (Project Maven) для анализа видео с дронов с помощью ИИ[5].

---

[1] abc.xyz
[2] reuters.com/article/us-usa-election-google-idUSKCN1ML1WJ
[3] nytimes.com/interactive/2019/06/08/technology/youtube-radical.html
[4] theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[5] nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html

X Corp

X Corp[1] – американская компания, основанная в 2006 году как Twitter, Inc. и переименованная в 2023 году после приобретения Илоном Маском. Штаб-квартира находится в Сан-Франциско, Калифорния. Управляет социальной платформой X, которая позволяет пользователям публиковать короткие сообщения, взаимодействовать с контентом и получать персонализированные рекомендации. В 2024 году X Corp сообщила о 500 млн активных пользователей ежемесячно.

Продукты и инструменты: платформа X, X API, X Ads, алгоритмы рекомендаций, X Premium.

Области применения в социальном управлении и влиянии: анализ цифровых следов, психографический анализ, социокультурный анализ, анализ поведения, таргетированная пропаганда, манипуляция рекомендательными системами, использование ботов.

Описание и примеры:

– Анализ цифровых следов: X собирает данные о постах, лайках, репостах и поисковых запросах пользователей для создания профилей. Пример: использование X API для анализа пользовательских взаимодействий в маркетинговых исследованиях[2].

– Психографический анализ: алгоритмы X анализируют посты и взаимодействия для определения интересов и предпочтений. Пример: таргетинг рекламы на основе анализа пользовательских твитов[3].

– Анализ поведения: платформа отслеживает, как пользователи взаимодействуют с контентом, чтобы оптимизировать рекомендации. Пример: мониторинг кликов и времени просмотра для улучшения UX в 2024 году[4].

– Таргетированная пропаганда: X позволяет рекламодателям настраивать кампании на основе демографии и интересов. Пример: использование X Ads для политической рекламы во время выборов в США 2024 года[5].

– Манипуляция рекомендательными системами: алгоритмы X продвигают контент, увеличивая вовлеченность, что может усиливать поляризацию. Пример: изменение алгоритмов в 2023 году привело к росту вирусного контента.[6]

– Использование ботов: боты на платформе X используются для автоматизации постов и влияния на тренды. Пример: развертывание ботов для информационных кампаний[7].

---

[1] x.com
[2] developer.x.com/en/docs/x-api
[3] blog.hootsuite.com/twitter-algorithm/
[4] ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance
[5] forbes.com/sites/stephenpastis/2024/10/07/could-republican-ties-to-x-impact-voters-heres-what-experts-say-as-trump-outspends-harris-on-the-site/
[6] theguardian.com/technology/2025/jan/17/eu-asks-x-for-internal-documents-about-algorithms-as-it-steps-up-investigation
[7] nbcnews.com/tech/internet/republican-bot-campaign-trump-x-twitter-elon-musk-fake-accounts-rcna173692

Amazon

Amazon.com, Inc.[1] – американская компания, основанная в 1994 году, со штаб-квартирой в Сиэтле, Вашингтон. Крупнейшая в мире платформа электронной коммерции, также предоставляет облачные услуги (AWS), стриминг (Prime Video) и решения в области ИИ. Занимается логистикой, розничной торговлей и производством устройств (Kindle, Echo). Публичная компания (NASDAQ: AMZN).

Продукты и инструменты: Amazon Web Services (AWS), включая сервисы облачных вычислений (EC2, S3), аналитические инструменты (Amazon Rekognition, SageMaker), Alexa для анализа голосовых данных и алгоритмы персонализации контента для рекомендаций.

Области применения в социальном управлении и влиянии: анализ цифровых следов, массовая слежка, анализ психографики и поведения, персонализация политического контента, социальное моделирование и прогнозирование.

Описание и примеры:

– Анализ цифровых следов: AWS предоставляет инструменты для анализа больших данных, включая поведение пользователей в интернете. Пример: AWS использовался ФБР для анализа данных из соцсетей и других источников для отслеживания подозреваемых в рамках программы PRISM, раскрытой Сноуденом[2].

– Массовая слежка: Amazon Rekognition используется для распознавания лиц и анализа изображений, что помогает в мониторинге общественных мест. Пример: сотрудничество с полицией США для анализа видеопотоков с камер наблюдения, вызвавшее критику за нарушение приватности[3].

– Анализ психографики и поведения: алгоритмы персонализации Amazon собирают данные о предпочтениях пользователей, которые могут быть использованы для таргетинга. Пример: использование данных покупок и просмотров для создания психографических профилей, что потенциально применимо в политической рекламе[4].

– Персонализация политического контента: рекомендательные системы Amazon могут продвигать определенный контент, влияя на восприятие. Пример: таргетированная реклама на Amazon Ads, используемая для продвижения политических кампаний в США[5].

– Социальное моделирование и прогнозирование: SageMaker позволяет создавать модели для прогнозирования поведения групп. Пример: использование Пентагоном AWS для анализа данных о социальных трендах в военных операциях[6].

---

[1] amazon.com
[2] theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[3] washingtonpost.com/technology/2020/06/10/amazon-rekognition-police/
[4] nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html
[5] cnbc.com/2021/03/29/amazons-pr-campaign-ahead-of-union-vote-shows-how-worried-it-is.html
[6] dailymail.co.uk/sciencetech/article-4889092/Amazon-authorized-host-DoD-s-sensitive-data.html

Microsoft

Microsoft Corporation [1] – американская технологическая компания, основанная в 1975 году, со штаб-квартирой в Редмонде, Вашингтон. Ведущий разработчик программного обеспечения (Windows, Office, Azure), облачных сервисов и аппаратного обеспечения (Surface, Xbox). Обслуживает корпоративный и потребительский рынки, активно развивает ИИ и квантовые вычисления. Публичная компания (NASDAQ: MSFT).

Продукты и инструменты: Microsoft Azure, Azure Cognitive Services, Dynamics 365, Microsoft Graph, LinkedIn (принадлежит Microsoft) и алгоритмы анализа данных для таргетинга и профилирования.

Области применения в социальном управлении и влиянии: анализ цифровых следов, массовая слежка, социальное моделирование и прогнозирование, таргетированная пропаганда, анализ психографики и поведения.

Описание и примеры:

– Анализ цифровых следов: Azure и Microsoft Graph собирают данные о пользователях через облачные сервисы и приложения (Office 365, LinkedIn). Пример: использование Azure АНБ для анализа метаданных пользователей в рамках программы PRISM[2].

– Массовая слежка: Azure предоставляет инфраструктуру для хранения и обработки данных разведки. Пример: контракт Microsoft с Пентагоном (JEDI) для облачного хранения данных, включая разведданные[3].

– Социальное моделирование и прогнозирование: Azure Cognitive Services анализируют поведение групп для прогнозирования социальных трендов. Пример: использование Azure для анализа общественных настроений[4].

– Таргетированная пропаганда: LinkedIn и Dynamics 365 позволяют таргетировать профессиональные аудитории. Пример: использование LinkedIn для распространения политической рекламы[5].

– Анализ психографики и поведения: Microsoft Graph создает профили пользователей на основе их активности. Пример: сотрудничество с ЦРУ для анализа данных сотрудников через Azure, раскрытое в утечках[6].

---

[1] microsoft.com
[2] theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[3] nytimes.com/2019/10/25/technology/dod-jedi-contract.html
[4] redwerk.com/blog/microsoft-azure-cognitive-services/
[5] campaigninginfo.com/how-to-use-linkedin-for-political-campaigns/
[6] bloomberg.com/politics/articles/2018-05-16/microsoft-wins-lucrative-cloud-deal-with-intelligence-community

IBM

International Business Machines Corporation (IBM)[1] – американская компания, основанная в 1911 году, со штаб-квартирой в Армонке, Нью-Йорк. Специализируется на ИТ-услугах, облачных вычислениях, искусственном интеллекте (Watson) и аппаратном обеспечении (квантовые компьютеры). Обслуживает предприятия более чем в 170 странах. Публичная компания (NYSE: IBM).

Продукты и инструменты: IBM Cloud, Watson AI, IBM Security Intelligence (QRadar), SPSS для статистического анализа, и IBM Marketing Cloud.

Области применения в социальном управлении и влиянии: анализ цифровых следов, массовая слежка, социальное моделирование и прогнозирование, таргетированная пропаганда, анализ психографики и поведения.

Описание и примеры:

– Анализ цифровых следов: Watson AI и QRadar собирают и анализируют данные из открытых и закрытых источников. Пример: Использование QRadar ФБР для отслеживания киберугроз через анализ активности в соцсетях[2].

– Массовая слежка: IBM Cloud предоставляет инфраструктуру для обработки больших объёмов данных разведки. Пример: Контракт IBM с ЦРУ для облачного хранения и анализа разведданных[3].

– Социальное моделирование и прогнозирование: SPSS и Watson используются для прогнозирования социальных трендов. Пример: использование Пентагоном Watson для когнитивных вычислений[4].

– Таргетированная пропаганда: IBM Marketing Cloud позволяет создавать таргетированные кампании. Пример: использование IBM для продвижения политической рекламы[5].

– Анализ психографики и поведения: Watson создает профили пользователей на основе их данных. Пример: сотрудничество с АНБ для анализа пользовательских данных в рамках PRISM[6].

---

[1] ibm.com
[2] habr.com/ru/companies/muk/articles/325330/
[3] fedscoop.com/cia-quietly-awards-billion-dollar-c2e-cloud-contract/
[4] datacenterdynamics.com/en/analysis/enlisting-watson-ibm-on-winning-us-army-private-cloud-contracts/
[5] forbes.ru/reklama/298629-ibm-marketing-cloud-oblachnyi-otvet-na-zaprosy-rynka
[6] theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Oracle

Oracle Corporation[1] – американская компания, основанная в 1977 году, со штаб-квартирой в Остине, Техас. Специализируется на разработке баз данных, облачных решений, ERP-систем и программного обеспечения для управления бизнесом. Один из крупнейших поставщиков корпоративных ИТ-решений, включая Oracle Database и Cloud Infrastructure. Публичная компания (NYSE: ORCL).

Продукты и инструменты: Oracle Cloud Infrastructure (OCI), Oracle Data Cloud, Marketing Cloud и инструменты анализа больших данных (Oracle Analytics Cloud).

Области применения в социальном управлении и влиянии: анализ цифровых следов, массовая слежка, таргетированная пропаганда, анализ психографики и поведения.

Описание и примеры:

– Анализ цифровых следов: Oracle Data Cloud собирает данные о поведении пользователей из множества источников. Пример: компания Oracle выплатила 115 млн долларов, чтобы урегулировать судебный иск, в котором ее, занимающуюся программным обеспечением для баз данных и облачными вычислениями, обвиняли во вторжении в частную жизнь людей путем сбора их личной информации и продажи ее третьим лицам[2].

– Массовая слежка: OCI предоставляет инфраструктуру для хранения и обработки разведданных. Пример: контракт Oracle с ЦРУ для облачного хранения данных разведки[3].

– Таргетированная пропаганда: Marketing Cloud позволяет создавать таргетированные кампании на основе данных пользователей. Пример: использование Oracle Marketing Cloud для политической рекламы в кампании 2020 года в США[4].

– Анализ психографики и поведения: Oracle Analytics Cloud создает психографические профили. Пример: использование Oracle для анализа поведения избирателей[5].

[1] oracle.com
[2] investing.com/news/stock-market-news/oracle-reaches-115-million-consumer-privacy-settlement-3527333
[3] fedscoop.com/cia-quietly-awards-billion-dollar-c2e-cloud-contract/
[4] adweek.com/programmatic/why-oracle-advertising-is-really-shutting-down/
[5] rittmanmead.com/blog/2017/02/analysing-elections-data-with-oracle-data-visualisation-desktop/

Salesforce

Salesforce, Inc.[1] – американская компания, основанная в 1999 году, со штаб-квартирой в Сан-Франциско, Калифорния. Лидер в области облачных CRM-решений (управление взаимоотношениями с клиентами), предоставляет платформы для автоматизации продаж, маркетинга и клиентского обслуживания. Обслуживает компании всех размеров в различных отраслях. Публичная компания (NYSE: CRM).

Продукты и инструменты: Salesforce Marketing Cloud, Einstein AI, Tableau для визуализации данных, и Salesforce Social Studio для анализа социальных сетей.

Области применения в социальном управлении и влиянии: таргетированная пропаганда, анализ цифровых следов, анализ психографики и поведения, манипуляция рекомендательными системами.

Описание и примеры:

– Таргетированная пропаганда: Marketing Cloud позволяет создавать персонализированные кампании. Пример: использование Salesforce для таргетинга политической рекламы[2].

– Анализ цифровых следов: Social Studio анализирует данные из соцсетей для профилирования. Пример: использование Salesforce для анализа цифровых следов клиентов компаний[3].

– Анализ психографики и поведения: Einstein AI создает психографические профили на основе пользовательских данных. Пример: применение Einstein для анализа предпочтений пользователей в политических кампаниях[4].

– Манипуляция рекомендательными системами: Marketing Cloud продвигает контент для повышения вовлеченности. Пример: продвижение поляризующего контента во время выборов[5].

---

[1] salesforce.com
[2] ethans.co.in/blogs/elevate-your-marketing-strategy-with-salesforce/
[3] translated.turbopages.org/proxy_u/en-ru.ru.f558ddf9-685bae2c-ace9b101-74722d776562/https/tutorialspoint.com/salesforce-integration-with-social-media-maximizing-your-reach
[4] slaesforce-faq.com/do-political-campaign-s-use-salesforce
[5] rolustech.com/blog/content-strategy-salesforce-marketing-cloud

Adobe

Adobe Inc.[1] – американская компания, основанная в 1982 году, со штаб-квартирой в Сан-Хосе, Калифорния. Ведущий разработчик программного обеспечения для креативных и маркетинговых решений, включая Photoshop, Acrobat и Experience Cloud. Специализируется на инструментах для дизайна, обработки документов и цифрового маркетинга. Публичная компания (NASDAQ: ADBE).

Продукты и инструменты: Adobe Experience Cloud, Adobe Analytics, Adobe Target, Adobe Campaign.

Области применения в социальном управлении и влиянии: анализ цифровых следов, психографический анализ, таргетированная пропаганда, информационные кампании.

Описание и примеры:

– Анализ цифровых следов: Adobe Analytics собирает данные о поведении пользователей на веб-сайтах и в приложениях. Пример: использование Analytics для анализа потребительских предпочтений в розничной торговле[2].

– Психографический анализ: Adobe Target создает профили пользователей для персонализации. Пример: применение Target для изучения поведения клиентов в банковском секторе[3].

– Таргетированная пропаганда: Adobe Campaign доставляет персонализированные маркетинговые сообщения. Пример: возможности Campaign позволяют использовать продукт для политической пропаганды. Имеются прецеденты.[4]

– Информационные кампании: Adobe Experience Cloud позволяет координировать кампании влияния. Пример: применение Experience Cloud для продвижения контента[5].

[1] adobe.com
[2] business.adobe.com/products/adobe-analytics.html
[3] news.adobe.com/news/news-details/2022/adobe-to-help-u-s-bank-accelerate-personalization-in-consumer-banking
[4] wsj.com/articles/adobe-plans-to-ban-political-ads-on-its-online-ad-sales-platform-11596222336
[5] firebearstudio.com/blog/adobe-experience-cloud.html

OpenAI

OpenAI [1] – американская компания, основанная в 2015 году, со штаб-квартирой в Сан-Франциско, Калифорния. Занимается разработкой искусственного интеллекта (ИИ), стремясь создать безопасный и полезный искусственный общий интеллект (AGI). Известна благодаря ChatGPT и моделям GPT, которые вызвали бум генеративного ИИ. В 2024 году OpenAI обслуживала более 500 млн активных пользователей еженедельно.

Продукты и инструменты: ChatGPT, GPT-4o, GPT-4.5, DALL·E 3, Whisper, Sora, OpenAI API, Codex (встроен в GitHub Copilot), Embeddings, Fine-Tuning Tools.

Области применения в социальном управлении и влиянии: анализ цифровых следов, психографический анализ, социокультурный анализ, анализ поведения, таргетированная пропаганда, социальное моделирование и прогнозирование, информационные кампании и PSYOP, использование ботов.

Описание и примеры:

– Анализ цифровых следов: OpenAI API позволяет анализировать текстовые данные, включая социальные сети и отзывы, для выявления трендов и предпочтений. Пример: компании используют OpenAI для анализа клиентских отзывов в соцсетях[2].

– Психографический анализ: модели OpenAI, такие как GPT-4o, анализируют текстовые данные для сегментации аудитории по интересам и ценностям. Пример: использование ChatGPT для анализа психографических данных из соцсетей[3].

– Социокультурный анализ: инструменты OpenAI выявляют культурные тренды через анализ текстов. Пример: использование ChatGPT для анализа социокультурных особенностей аудитории[4].

– Анализ поведения: OpenAI анализирует поведение пользователей через обработку больших массивов данных. Пример: использование предиктивной аналитики GPT для прогнозирования предпочтений на основе истории поиска и кликов[5].

– Таргетированная пропаганда: OpenAI API используется для создания целевого контента, который влияет на аудиторию. Пример: OpenAI выявляет и блокирует китайские операции, использующие ChatGPT для создания пропагандистских постов на X и TikTok[6].

– Социальное моделирование и прогнозирование: модели OpenAI прогнозируют тренды и поведение на основе исторических данных. Пример: в 2023

---

[1] openai.com
[2] prodelo.biz/uslugi-opencart/stsenarii-avtomatizatsii/n8n/analiz-postov-na-reddit-s-pomoschyu-ii-dlya-poiska-biznes-vozmozhnostey
[3] vc.ru/telegram/1675482-zabud-o-kastdevah-i-nachni-analizirovat-svoyu-auditoriyu-pri-pomoshi-chat-gpt-dazhe-esli-net-bloga
[4] aistrata.tech/mclasses/tpost/eedtnzmzv1-marketing-po-novomu-vliyanie-chatgpt-na
[5] openaisuite.com/predictive-analytics-forecasting-the-future-with-big-data/
[6] deepnewz.com/china/openai-bans-chinese-sneer-review-operation-using-chatgpt-influence-campaigns-1e14008e

году компании применяли OpenAI API для прогнозирования спроса на продукты, анализируя социальные медиа и продажи[1].

– Информационные кампании и PSYOP: инструменты OpenAI использовались в кампаниях влияния, включая государственные операции. Пример: OpenAI пресекает операции влияния ряда стран (Россия, Китай, Иран), использовавших ChatGPT для создания постов, комментариев и биографий для манипуляции общественным мнением[2].

– Использование ботов: ChatGPT и API позволяют создавать ботов для автоматизации взаимодействия. Пример: OpenAI заблокировала российскую операцию, использовавшую ChatGPT для создания Telegram-ботов с политическими комментариями[3].

[1] spaceotechnologies.com/blog/how-to-use-openai-for-business-data-analysis/
[2] npr.org/2025/06/05/nx-s1-5423607/openai-china-influence-operations
[3] d11jmx241r4rky.cloudfront.net/a/open-ai-rossiya-seti-vliyaniya/32973869.html

Leidos

Leidos Holdings, Inc.[1] – американская компания, основанная в 1969 году как Science Applications International Corporation (SAIC), со штаб-квартирой в Рестоне, Вирджиния. Специализируется на информационных технологиях, обороне, авиации и биомедицинских исследованиях. Крупнейший поставщик ИТ-услуг для оборонного сектора США после слияния с IT-подразделением Lockheed Martin в 2016 году. Публичная компания (NYSE: LDOS).

Продукты и инструменты: Security Enterprise Solutions (SES), Integrated Wide Area Surveillance System (IWASS), Foundational Automation Support Technology (FAST), SkyLine-X™.

Области применения в социальном управлении и влиянии: анализ цифровых следов, психографический анализ, массовая слежка.

Описание и примеры:

– Анализ цифровых следов: Security Enterprise Solutions (SES) использует AI и биометрические технологии для сбора и анализа данных о поведении людей и грузов. Пример: применение SES для анализа данных пассажиров в аэропортах США для повышения безопасности[2].

– Психографический анализ: FAST framework применяет AI и машинное обучение для создания профилей на основе аномалий в поведении пользователей. Пример: участие Leidos в обнаружении инсайдерских угроз в сетях Пентагона[3].

– Массовая слежка: Integrated Wide Area Surveillance System (IWASS) обеспечивает мониторинг границ и критической инфраструктуры. Пример: развертывание IWASS для пограничного контроля.[4]

[1] leidos.com
[2] leidos.com/markets/aviation/security-detection
[3] leidos.com/sites/leidos/files/2023-02/Leidos-Zero-Trust%20Pentagon-DD.pdf
[4] leidos.com/products

Amentum

Amentum Holdings, Inc.[1] – американский подрядчик в сфере государственных и коммерческих услуг, основанный в 2020 году как спин-офф подразделения AECOM, со штаб-квартирой в Шантильи, Вирджиния. Предоставляет услуги в области управления объектами, ядерной безопасности и обучения военных. Второй по величине подрядчик государственных услуг в США после Leidos. Публичная компания с 2024 года (NYSE: AMTM).

Продукты и инструменты: Data Analytics Center of Excellence (CoE), PPMx, Intelligence, Surveillance, and Reconnaissance (ISR) Solutions, Counterintelligence Capabilities.

Области применения в социальном управлении и влиянии: анализ цифровых следов, массовая слежка, защита от шпионажа.

Описание и примеры:

– Анализ цифровых следов: Data Analytics CoE использует AI и машинное обучение для обработки больших данных из различных источников, включая HUMINT, SIGINT и OSINT, для создания actionable insights. Пример: применение CoE для анализа данных в интересах национальной безопасности США[2].

– Массовая слежка: ISR Solutions интегрируют многофункциональные сенсоры для реального времени мониторинга и анализа угроз. Пример: развертывание ISR для поддержки разведывательных операций Министерства обороны США[3].

– Защита от шпионажа: Counterintelligence Capabilities используют автоматизированные технологии для нейтрализации угроз и управления информационными потоками. Пример: использование Counterintelligence для защиты от шпионажа Пентагона[4].

[1] amentum.com
[2] amentum.com/our-capabilities/data-analytics-and-cyber/
[3] amentum.com/markets/intelligence/
[4] amentum.com/our-capabilities/data-analytics-and-cyber/counter-intelligence-solutions/

Kratos Defense and Security Solutions

Kratos Defense & Security Solutions, Inc.[1] – американская технологическая компания, основанная в 1994 году как Wireless Facilities Incorporated, со штаб-квартирой в Сан-Диего, Калифорния. Специализируется на военных технологиях, включая беспилотные системы, спутниковую связь и электронику. Обслуживает правительство США, иностранные правительства и коммерческих клиентов.

Продукты и инструменты: OpenSpace Platform, Cyber Fusion Operations, Mixed Reality (MR) Training Systems, C5ISR Solutions.

Области применения в социальном управлении и влиянии: анализ цифровых следов, массовая слежка, спутниковая разведка.

Описание и примеры:

– Анализ цифровых следов: Cyber Fusion Operations используют AI для анализа данных из сетей и устройств, выявляя угрозы и аномалии. Пример: применение Cyber Fusion Operations для анализа киберугроз в интересах Министерства обороны США[2].

– Массовая слежка: C5ISR Solutions интегрируют сенсоры и системы для мониторинга в реальном времени, включая спутниковую разведку и беспилотные системы. Пример: развертывание C5ISR для поддержки разведывательных операций ВВС США[3].

– Спутниковая разведка: OpenSpace Platform координирует спутниковые коммуникации, обеспечивая управление информационными потоками. Пример: использование OpenSpace для создания центрального облачного командного центра спутниковых систем[4].

[1] kratosdefense.com
[2] kratoscyber.com/
[3] kratosdefense.com/
[4] asdnews.com/news/defense/2023/05/03/kratos-takes-multimission-satellite-ground-system-support-demo-road

Raytheon

Raytheon [1] – подразделение RTX Corporation, американский оборонный подрядчик, основанный в 1922 году, со штаб-квартирой в Арлингтоне, Вирджиния. Специализируется на производстве оружия, военной и коммерческой электроники, включая управляемые ракеты (Patriot, Sparrow), радары и системы кибербезопасности. Является одним из крупнейших оборонных подрядчиков США, получая более 90% доходов от военных контрактов. В 2020 году объединился с United Technologies, образовав RTX Corporation.

Продукты и инструменты: Rapid Information Overlay Technology (RIOT), Cyber Fusion Operations, C5ISR Solutions, AXON Enterprise Operation Centre.

Области применения в социальном управлении и влиянии: анализ цифровых следов, массовая слежка, операции влияния.

Описание и примеры:

– Анализ цифровых следов: RIOT анализирует данные из социальных сетей для создания профилей и прогнозирования поведения. Пример: использование RIOT для сбора данных о перемещениях и связях лиц в интересах разведки США[2].

– Массовая слежка: C5ISR Solutions интегрируют сенсоры, спутниковые данные и системы реального времени для мониторинга угроз. Пример: развертывание C5ISR для поддержки разведывательных операций ВВС США[3].

– Операции влияния: AXON Enterprise Operation Centre координирует информационные потоки и поддерживает управление операциями в киберпространстве. Пример: использование AXON для поддержки операций Министерства обороны США[4].

[1] rtx.com
[2] zdnet.com/article/raytheon-riot-defense-spying-is-coming-to-social-networks/
[3] en.wikipedia.org/wiki/Raytheon
[4] raytheon.co.uk/what-we-do/cyber-space-and-training/mission-intelligence

Lockheed Martin

Lockheed Martin[1] – американская аэрокосмическая и оборонная компания, основанная в 1995 году путем слияния Lockheed Corporation и Martin Marietta, со штаб-квартирой в Северном Бетесде, Мэриленд. Крупнейший подрядчик правительства США, специализируется на разработке военных самолетов (F-35, F-16), ракетных систем, космических технологий (Orion) и кибербезопасности. Публичная компания (NYSE: LMT).

Продукты и инструменты: Cyber Kill Chain, Semantic Forensics (SemaFor), AI Factory, Lockheed Martin AI Center (LAIC), Integrated Intelligence Surveillance Reconnaissance Systems (ISR).

Области применения в социальном управлении и влиянии: анализ цифровых следов, массовая слежка, социальное моделирование и прогнозирование, операции влияния, PSYOP.

Описание и примеры:

– Анализ цифровых следов: Cyber Kill Chain анализирует цифровые следы для выявления и предотвращения кибератак, отслеживая этапы от разведки до выполнения. Пример: использование Cyber Kill Chain для анализа кибератаки на Equifax в 2017 году с выявлением уязвимостей в Apache Struts[2].

– Массовая слежка: ISR-системы собирают данные с дронов, спутников и наземных станций для мониторинга в реальном времени. Пример: использование Airborne Multi-INT Lab (AML) для временного развертывания разведки в зонах конфликтов[3].

– Социальное моделирование и прогнозирование: AI Factory и LAIC используют ИИ для прогнозирования угроз и моделирования сценариев. Пример: применение AI Factory для прогнозирования военных угроз и перемещений людей, включая анализ данных со спутников[4].

– Операции влияния: SemaFor выявляет и противодействует дезинформации в медиа и поддерживает собственные информационные операции. Пример: разработка прототипа SemaFor для DARPA[5].

– PSYOP: AI Factory разрабатывает ИИ-решения для психологических операций. Пример: дистанционный нейронный мониторинг, используемый в неэтичных армейских экспериментах PSYOP[6].

---

[1] lockheedmartin.com
[2] adesso.de/en/news/blog/cyber-kill-chain.jsp
[3] lockheedmartin.com/en-us/products/integrated-intelligence-surveillance-reconnaissance-systems.html
[4] aimresearch.co/market-industry/from-seaplanes-to-ai-how-lockheed-martin-transformed-defense-and-aerospace
[5] truth11.com/semantic-forensics-semafor-darpas-new-mass-surveillance-disinformation-control-tool/
[6] huffpost.com/entry/remote-neural-monitoring-used-in-unethical-army-psyop_b_587fe170e4b0fb40bf6c462a

Northrop Grumman

Northrop Grumman Corporation [1] – американская многонациональная аэрокосмическая и оборонная компания, основанная в 1994 году путем покупки Grumman Aerospace корпорацией Northrop. С 97 000 сотрудников и годовым доходом более 40 млрд долларов это один из крупнейших производителей оружия и поставщиков военных технологий в мире. Компания разрабатывает передовые системы для космоса, авиации, обороны и киберпространства, включая B-21 Raider и системы разведки. В 2022 году она занимала третье место среди оборонных подрядчиков мира и 101-е место в списке Fortune 500.

Продукты и инструменты: Deep Sensing and Targeting (DSaT), Advanced Battle Manager (ABM), Forward Area Air Defense (FAAD), Cyber Intelligence Systems, Airborne Intelligence, Surveillance, and Reconnaissance (ISR) Systems, Beacon.

Области применения в социальном управлении и влиянии: массовая слежка, анализ цифровых следов, социальное моделирование и прогнозирование, информационные кампании.

Описание и примеры:

– Массовая слежка: системы Airborne ISR и DSaT собирают данные с воздуха и из космоса для мониторинга в реальном времени. Пример: демонстрация DSaT армии США для разведки за пределами прямой видимости[2].

– Анализ цифровых следов: Cyber Intelligence Systems анализируют цифровые следы для выявления киберугроз. Пример: использование киберсистем для защиты данных Пентагона от атак через анализ цифровых следов[3].

– Информационные кампании: ИИ-системы, такие как Beacon, создают контент и ботов. Пример: Northrop Grumman презентовала экосистему нового поколения для обеспечения новых возможностей автономных миссий Beacon, которая представляет собой интегрированную среду, имитирующую соответствующие сценарии миссий[4].

[1] northropgrumman.com
[2] epicos.com/article/880407/northrop-grummans-deep-sensing-and-targeting-technology-goes-airborne-advance-vision
[3] web.archive.org/web/20230321051530/northropgrumman.com/cyber/
[4] designdevelopmenttoday.com/industries/aerospace/news/22943995/northrop-grumman-unveils-autonomous-testbed-ecosystem

General Dynamics

General Dynamics Corporation[1] – американская аэрокосмическая и оборонная компания, основанная в 1952 году в результате слияния Electric Boat и Canadair. Штаб-квартира находится в Рестоне, Вирджиния. Компания является пятым по величине оборонным подрядчиком в мире по объему продаж оружия и пятым в США по общему объему продаж с доходом в 47,7 млрд долларов в 2024 году и штатом около 117 000 сотрудников. General Dynamics разрабатывает продукцию в области бизнес-авиации, боевых систем, информационных технологий и кораблестроения, включая самолеты Gulfstream, подводные лодки классов Virginia и Columbia, эсминцы класса Arleigh Burke, танки M1 Abrams и бронемашины Stryker.

Продукты и инструменты: Cyber Defense Solutions, Mission Command and Control Systems, Intelligence, Surveillance, and Reconnaissance (ISR) Systems, Integrated Mission Systems, Prophet SIGINT Systems, Secure Communications.

Области применения в социальном управлении и влиянии: массовая слежка, анализ цифровых следов, социальное моделирование и прогнозирование.

Описание и примеры:

– Массовая слежка: ISR-системы и Prophet SIGINT собирают данные с помощью сигналов разведки (SIGINT) и электронных систем для мониторинга в реальном времени. Пример: использование Prophet SIGINT для перехвата коммуникаций[2].

– Анализ цифровых следов: Cyber Defense Solutions анализируют цифровые следы для выявления киберугроз и защиты данных. Пример: применение Cyber Defense Solutions для защиты инфраструктуры Пентагона через анализ цифровых следов[3].

– Социальное моделирование и прогнозирование: Mission Command and Control Systems используют ИИ для моделирования военных сценариев и прогнозирования угроз. Пример: интеграция ИИ в системы управления для военных симуляций[4].

[1] gd.com
[2] web.archive.org/web/20080417031944/http://findarticles.com/p/articles/mi_m0IBS/is_3_26/ai_67544226
[3] gdmissionsystems.com/cyber
[4] diversedaily.com/command-and-control-simulation-understanding-algorithms-for-war-simulations/

Clearview AI

Clearview AI[1] – американская компания, основанная в 2017 году Хоаном Тон-Татом и Ричардом Шварцем, со штаб-квартирой в Нью-Йорке. Специализируется на технологиях распознавания лиц для правоохранительных органов и частных организаций. В 2024 году база данных компании включала более 50 млрд изображений лиц, а ее клиентами являются тысячи агентств по всему миру.

Продукты и инструменты: Clearview AI Facial Recognition, база данных изображений лиц, мобильное приложение для идентификации в реальном времени.

Области применения в социальном управлении и влиянии: массовая слежка, анализ цифровых следов, анализ поведения.

Описание и примеры:

– Массовая слежка: Clearview AI собирает миллиарды изображений из публичных источников, таких как социальные сети, для создания базы данных, используемой для идентификации лиц. Пример: технология использовалась полицией США для идентификации подозреваемых на основе уличных камер[2].

– Анализ цифровых следов: Система сопоставляет лица с профилями в социальных сетях, извлекая данные о местоположении и активности. Пример: в 2021 году Clearview AI помогла идентифицировать участников протестов в США, используя их цифровые следы[3].

– Анализ поведения: данные из социальных сетей и геолокации используются для прогнозирования поведения и отслеживания перемещений. Пример: технология применялась для мониторинга перемещений подозреваемых в реальном времени правоохранительными органами[4].

[1] clearview.ai
[2] washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/
[3] nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html?ysclid=mcbsazt6rv719969351
[4] appercase.ru/news/9532/

Cision

Cision[1] – глобальная компания, основанная в 1867 году, со штаб-квартирой в Чикаго, Иллинойс. Специализируется на программном обеспечении и услугах для PR, маркетинга и мониторинга СМИ. Обслуживает более 75 000 клиентов по всему миру, включая бренды, агентства и медиа. В 2024 году Cision приобрела Brandwatch, усилив свои возможности в анализе социальных сетей.

Продукты и инструменты: Cision Communications Cloud, Cision Connect, Brandwatch, Cision Social Listening, Cision Analytics, PR Newswire.

Области применения в социальном управлении и влиянии:

Анализ цифровых следов, психографический анализ, социокультурный анализ, таргетированная пропаганда.

Описание и примеры:

– Анализ цифровых следов: Cision использует инструменты, такие как Brandwatch, для отслеживания упоминаний брендов, хештегов и активности пользователей в социальных сетях. Пример: анализ упоминаний компании в социальных сетях для оценки репутации в 2024 году[2].

– Психографический анализ: Cision анализирует предпочтения и интересы аудитории на основе данных социальных сетей для создания персонализированных кампаний. Пример: использование Brandwatch для таргетинга рекламы на основе эмоциональных реакций пользователей[3].

– Социокультурный анализ: инструменты Cision выявляют тренды и общественные настроения через анализ контента в СМИ и соцсетях. Пример: исследование хештегов для выявления экологических трендов[4].

– Таргетированная пропаганда: Cision помогает создавать целевые PR-кампании, используя данные об аудитории для влияния на общественное мнение. Пример: распространение пресс-релизов через PR Newswire для продвижения корпоративных инициатив[5].

[1] cision.com
[2] brandwatch.com/blog/social-media-monitoring/
[3] fastercapital.com/ru/content/Ultimate-FAQ--Brandwatch--что--как--почему--когда.html
[4] brandwatch.com/blog/marketing-brand-sustainability-effectively/
[5] cision.nl/en/prnewswire/

Sprout Social

Sprout Social[1] – американская компания, основанная в 2010 году, со штаб-квартирой в Чикаго, Иллинойс. Специализируется на управлении социальными сетями, предоставляя инструменты для планирования, мониторинга, аналитики и взаимодействия с аудиторией. В 2024 году платформа обслуживала более 30 000 брендов и агентств по всему миру.

Продукты и инструменты: Sprout Social Dashboard, Smart Inbox, Sprout Social Analytics, Social Listening, Premium Analytics, Employee Advocacy, Sprout Social Compose, Tableau BI Connector.

Области применения в социальном управлении и влиянии: анализ цифровых следов, психографический анализ, социокультурный анализ, анализ поведения, таргетированная пропаганда.

Описание и примеры:

– Анализ цифровых следов: Sprout Social отслеживает упоминания брендов, хештеги и взаимодействия в социальных сетях для создания детализированных профилей аудитории. Пример: использование Social Listening для мониторинга разговоров о бренде в социальных сетях[2].

– Психографический анализ: платформа анализирует интересы, предпочтения и эмоциональные реакции аудитории для персонализации контента[3].

– Социокультурный анализ: Sprout Social выявляет культурные тренды и общественные настроения через анализ разговоров в соцсетях. Пример: работы Sprout Social направлены на понимание потребностей аудитории, тенденций в онлайн-культуре[4].

– Анализ поведения: инструменты аналитики Sprout Social измеряют вовлеченность, клики и демографию аудитории для оптимизации стратегий. Пример: Penn State Health использовала тегирование в Sprout для повышения вовлеченности[5].

– Таргетированная пропаганда: Sprout Social поддерживает создание целевых кампаний на основе данных об аудитории для влияния на общественное мнение. Пример: использование Sprout Social Ads для таргетинга рекламы на LinkedIn для b2b-аудитории[6].

---

[1] sproutsocial.com
[2] sproutsocial.com/insights/social-media-monitoring/
[3] deswalsh.com/2012/04/25/testing-the-social-media-engagement-management-tool-sprout-social-part-2/
[4] sdelaem.agency/blog/tendenczii-v-kontent-marketinge-v-2024-issledovanie-sprout-social/
[5] sproutsocial.com/insights/case-studies/pennstatehealth/
[6] salespanel.io/resources/b2b-linkedin-ads/

Nielsen

Nielsen [1] – американская компания, основанная в 1923 году, со штаб-квартирой в Нью-Йорке. Является мировым лидером в области измерения аудитории, данных и аналитики, обслуживая медиа, рекламодателей и бренды более чем в 55 странах. В 2024 году Nielsen продолжала предоставлять информацию о потребительском поведении и медиапотреблении.

Продукты и инструменты: Nielsen Ratings, Nielsen Digital Ad Ratings, Nielsen Streaming Video Ratings, Nielsen Scarborough, Nielsen Consumer Panel (NCP), Nielsen ONE, Gracenote, Nielsen Analytics, PRIZM Premier, P$ycle, ConneXions.

Области применения в социальном управлении и влиянии: анализ цифровых следов, психографический анализ, социокультурный анализ, анализ поведения, таргетированная пропаганда, социальное моделирование и прогнозирование.

Описание и примеры:

– Анализ цифровых следов: Nielsen отслеживает цифровую активность пользователей через Nielsen Digital Ad Ratings и Streaming Video Ratings, измеряя просмотры и взаимодействия в интернете и на стриминговых платформах. Пример: в 2024 году Nielsen измерила просмотры фильма Deadpool & Wolverine на Disney+[2].

– Психографический анализ: Nielsen использует психографические данные для сегментации аудитории на основе мотиваций и предпочтений. Пример: Nielsen и CBS предложили модель шести сегментов аудитории, основанную на психографике, для повышения эффективности рекламы[3].

– Социокультурный анализ: Nielsen анализирует общественные тренды и культурные предпочтения через инструменты, такие как Nielsen Scarborough. Пример: анализ потребления контента поколения Z в 2023 году показал рост времени, проведенного в социальных сетях[4].

– Анализ поведения: Nielsen измеряет поведение потребителей через панели и аналитику, включая покупки и медиапотребление. Пример: National Consumer Panel отслеживает покупки в розничной торговле, связывая их с демографией домохозяйств[5].

– Таргетированная пропаганда: Nielsen помогает рекламодателям достигать целевых аудиторий с помощью точного таргетинга[6].

---

[1] nielsen.com
[2] fictionhorizon.com/deadpool-wolverine-dominates-nielsens-streaming-chart-in-its-disney-debut-week/
[3] translated.turbopages.org/proxy_u/en-ru.ru.325c09eb-685bd002-d2945693-74722d776562/https/ultimatepopculture.fandom.com/wiki/Nielsen_ratings
[4] nielsen.com/solutions/scarborough
[5] survey.money/blog/national-consumer-panel-review/
[6] nielsen.com/solutions/media-planning/audience-segments/

CrowdStrike

CrowdStrike [1] – американская компания в области кибербезопасности, основанная в 2011 году, со штаб-квартирой в Остине, Техас. Предоставляет облачные решения для защиты конечных устройств, облачных сред, идентификаций и данных. В 2024 году CrowdStrike обслуживает крупные предприятия, правительственные организации и малый бизнес по всему миру.

Продукты и инструменты: CrowdStrike Falcon Platform, Falcon Endpoint Protection, Falcon Insight XDR, Falcon Identity Threat Protection, Falcon Intelligence, Charlotte AI, Falcon LogScale, Falcon Foundry, CrowdStrike Threat Graph.

Области применения в социальном управлении и влиянии: анализ цифровых следов, анализ поведения, социальное моделирование и прогнозирование.

Описание и примеры:

– Анализ цифровых следов: CrowdStrike Falcon собирает и анализирует данные о действиях пользователей, системных логах и сетевом трафике для выявления угроз. Пример: в 2024 году Falcon Intelligence помог выявить действия хакерской группы LIMINAL PANDA[2].

– Анализ поведения: использует AI и машинное обучение для обнаружения аномалий в поведении пользователей и систем. Пример: Falcon Insight XDR выявил несанкционированные попытки аутентификации[3].

– Социальное моделирование и прогнозирование: CrowdStrike использует Threat Graph для анализа триллионов событий в реальном времени и прогнозирования киберугроз[4].

[1] crowdstrike.com
[2] all-about-security.de/unveiling-liminal-panda-a-closer-look-at-chinas-cyber-threats-to-the-telecom-sector/
[3] keepersecurity.com/blog/ru/2024/09/13/the-most-recent-credential-stuffing-attacks-on-companies-in-2024/
[4] dzen.ru/a/Z6sECzanbRLqUA7o

The Trade Desk

The Trade Desk[1] – американская технологическая компания, основанная в 2009 году, со штаб-квартирой в Вентуре, Калифорния. Специализируется на программатике и автоматизации маркетинга в реальном времени, предоставляя независимую платформу для покупки цифровой рекламы (demand-side platform). Компания обслуживает рекламодателей по всему миру, конкурируя с Google и Meta[2].

Продукты и инструменты: The Trade Desk DSP, Unified ID 2.0, Koa, Audience Insights.

Области применения в социальном управлении и влиянии: анализ цифровых следов, психографический анализ, таргетированная пропаганда.

Описание и примеры:

– Анализ цифровых следов: The Trade Desk DSP собирает данные о поведении пользователей через реальное время торгов (RTB) и интегрирует их с данными из CRM и сторонних источников. Пример: использование DSP для анализа потребительских предпочтений в розничной торговле США[3].

– Психографический анализ: Audience Insights и Koa используют AI для создания профилей пользователей на основе интересов, поведения и намерений покупки. Пример: применение Audience Insights для изучения поведения покупателей[4].

– Таргетированная пропаганда: The Trade Desk DSP поддерживает таргетинг по демографии, геолокации, интересам и кросс-девайсным данным. Пример: возможность использования DSP для политической рекламы[5].

[1] thetradedesk.com
[2] признана экстремистской и запрещённой на территории РФ
[3] thetradedesk.com/uk/our-demand-side-platform
[4] okocrm.com/blog/zachem-prognozirovat-povedenie-klientov/
[5] crossdevicemediagroup.com/audience-targeting-with-trade-desk/

Sprinklr

Sprinklr[1] – американская компания, основанная в 2009 году Рэги Томасом, со штаб-квартирой в Нью-Йорке. Разрабатывает платформу управления клиентским опытом (CXM) на основе SaaS, объединяющую маркетинг, рекламу, исследования, клиентскую поддержку и вовлеченность через 30+ цифровых каналов, включая социальные сети, мессенджеры, чат, CMC и email. В 2025 году Sprinklr обслуживал тысячи крупных предприятий по всему миру.

Продукты и инструменты: Sprinklr Social, Sprinklr Insights, Sprinklr Marketing, Sprinklr Service, Sprinklr AI+, Product Insights, Sprinklr Intuition, Employee Advocacy Platform, Social Listening Tools.

Области применения в социальном управлении и влиянии: анализ цифровых следов, психографический анализ, анализ поведения, таргетированная пропаганда, социальное прогнозирование.

Описание и примеры:

– Анализ цифровых следов: Sprinklr Insights собирает и анализирует данные из социальных сетей, отзывов и других источников для выявления клиентских настроений и трендов. Пример: в 2024 году крупная телекоммуникационная компания сократила время ответа в соцсетях на 70% благодаря автоматизированным уведомлениям Sprinklr Insights[2].

– Психографический анализ: Sprinklr использует AI для сегментации аудитории по ценностям, интересам и мотивациям. Пример: Sprinklr AI+ помогает брендам создавать персонализированные кампании, анализируя психографические данные из комментариев в соцсетях[3].

– Анализ поведения: платформа отслеживает поведение пользователей, включая взаимодействия и покупки, для прогнозирования потребностей. Пример: в 2024 году ритейлер использовал Sprinklr для анализа поведения клиентов[4].

– Социальное прогнозирование: Sprinklr использует предиктивную аналитику для прогнозирования трендов и поведения. Пример: в 2025 году Sprinklr Insights предсказала рост спроса на экологичные продукты, основываясь на исторических данных и трендах в соцсетях[5].

---

[1] sprinklr.com
[2] fragrancelounge-ea.com/blog/sprinklr-insights-real-time-insights-social/?v=518f4a738816
[3] sprinklr.com/stories/luxury-car-company/
[4] itrportal.com/articles/2024/06/25/sprinklr-named-a-leader-in-digital-customer-interaction-solutions-report/
[5] compositepanel.ru/news/detail/tendentsii-razvitiya-rynka-30-03-2025-14-46-04/

Snowflake

Snowflake Inc.[1] – американская компания, основанная в 2012 году, со штаб-квартирой в Бозмане, Монтана. Предоставляет облачную платформу AI Data Cloud для хранения, обработки и анализа данных, работающую на AWS, Microsoft Azure и Google Cloud. В 2024 году Snowflake обслуживала более 10 600 клиентов, включая 800+ компаний из Forbes Global 2000, обрабатывая 4,2 млрд запросов ежедневно.

Продукты и инструменты: Snowflake AI Data Cloud, Snowflake Cortex AI, Snowflake Intelligence, Snowflake ML, Snowpark, Streamlit, Snowflake Horizon Catalog, Customer Data Platform (CDP), Marketing Analytics, Audience Analysis Tools.

Области применения в социальном управлении и влиянии: анализ цифровых следов, психографический анализ, социокультурный анализ, анализ поведения, таргетированная пропаганда, социальное моделирование и прогнозирование.

Описание и примеры:

– Анализ цифровых следов: Snowflake собирает и анализирует данные с веб-сайтов, из социальных сетей, email-кампаний и других источников для создания 360-градусного профиля клиентов. Пример: в 2024 году ритейлер использовал Snowflake для анализа трафика веб-сайта и социальных взаимодействий, улучшив таргетинг рекламы[2].

– Психографический анализ: платформа позволяет сегментировать аудиторию по ценностям, убеждениям и интересам, используя данные из Snowflake Marketplace. Пример: маркетологи применяли Snowflake для создания персонализированных кампаний на основе психографических данных из соцсетей[3].

– Социокультурный анализ: Snowflake Insights анализирует данные для выявления культурных трендов и общественных настроений. Пример: в 2024 году медиакомпания использовала Snowflake для анализа трендов в контенте, адаптировав стратегию под аудиторию[4].

– Социальное моделирование и прогнозирование: Snowflake Cortex AI использует предиктивную аналитику для прогнозирования спроса и трендов. Пример: в 2024 году ритейлер прогнозировал спрос на товары в праздничный сезон с помощью Cortex, оптимизировав запасы[5].

---

[1] snowflake.com
[2] snowflake.com/en/the-modern-marketing-data-stack-report/
[3] appercase.ru/news/5457/
[4] analytikaplus.ru/kak-snowflake-pomogaet-brendam-personalizirovat-kontent-dlya-millionov-klientov/
[5] atlan.com/know/snowflake/snowflake-cortex-use-cases/

Recorded Future

Recorded Future[1] – американская компания в области кибербезопасности, основанная в 2009 году Кристофером Альбергом и Стаффаном Труве, со штаб-квартирой в Сомервилле, Массачусетс. Специализируется на разведке угроз (Threat Intelligence), используя ИИ и машинное обучение для анализа данных из открытых, глубоких и темных веб-источников. В 2024 году компания была приобретена MasterCard. Recorded Future обслуживает тысячи клиентов, включая крупные корпорации и государственные организации, предоставляя решения для прогнозирования и предотвращения киберугроз.

Продукты и инструменты: Recorded Future Intelligence Platform, Insikt Group, Temporal Analytics Engine, Recorded Future Social Media Intelligence, Threat Intelligence Feeds, Recorded Future Cortex AI, Vulnerability Intelligence, Brand Intelligence.

Области применения в социальном управлении и влиянии: анализ цифровых следов, социокультурный анализ, анализ поведения, социальное моделирование и прогнозирование.

Описание и примеры:

– Анализ цифровых следов: Recorded Future собирает и анализирует данные из открытых источников (OSINT), социальных сетей, форумов и темного веба для выявления цифровых следов, связанных с киберугрозами. Пример: платформа обнаружила утечку документации ВВС США через мониторинг даркнета[2].

– Социокультурный анализ: платформа анализирует общественные настроения и культурные тренды в социальных медиа для выявления потенциальных угроз. Пример: в 2022 году Recorded Future выявила китайскую дезинформационную кампанию в социальных сетях, направленную на американскую аудиторию[3].

– Анализ поведения: Recorded Future использует поведенческую аналитику для профилирования активности злоумышленников, включая тактики, техники и процедуры (TTP). Пример: компания помогла выявить аномальное поведение пользователей, связанное с фишинговыми атаками[4].

– Социальное моделирование и прогнозирование: Temporal Analytics Engine применяет предиктивную аналитику для прогнозирования киберугроз на основе исторических данных. Пример: Recorded Future предсказала рост атак на энергетический сектор, основываясь на трендах в даркнете[5].

---

[1] recordedfuture.com
[2] xakep.ru/2018/07/12/military-docs-leak/
[3] cyberscoop.com/chinese-disinformation-recorded-future/
[4] habr.com/ru/news/786422/
[5] datafloq.com/read/big-data-startup-review-recorded-future/

ShadowDragon

ShadowDragon[1] – американская компания, основанная в 2016 году Даниэлем Клеменсом как спин-офф его консалтинговой фирмы Packet Ninjas, со штаб-квартирой в штате Вайоминг. Специализируется на разработке программного обеспечения для разведки на основе открытых источников (OSINT), собирая и анализируя данные из социальных сетей, поверхностного, глубокого и темного веба. Список клиентов включает правоохранительные органы, государственные учреждения, военные организации и корпорации, такие как ICE, FBI и Massachusetts State Police.

Продукты и инструменты: SocialNet, Horizon, Horizon Monitor (ранее OIMonitor), Horizon Identity, Maltego Integration, OSINT APIs, Specialized Datasets.

Области применения в социальном управлении и влиянии: массовая слежка, анализ цифровых следов, социокультурный анализ, анализ поведения, социальное моделирование и прогнозирование, использование ботов.

Описание и примеры:

– Массовая слежка: ShadowDragon собирает данные из более чем 200 онлайн-источников, включая социальные сети (LinkedIn, Reddit, TikTok), приложения (Venmo, Tinder), игровые платформы (Fortnite) и сайты, такие как BabyCenter и PornHub, для мониторинга активности пользователей. Пример: Michigan State Police использовала ShadowDragon через контракт с Kaseware для создания системы криминальной разведки, отслеживая активность в интернете[2].

– Анализ цифровых следов: SocialNet и Horizon собирают публично доступные данные для построения профилей и связей между аккаунтами. Пример: правоохранительные органы использовали SocialNet для быстрого создания досье на подозреваемых, сопоставляя их email, псевдонимы и номера телефонов[3].

– Социокультурный анализ: Horizon Monitor анализирует социальные медиа для выявления настроений и трендов. Пример: корпорация использовала Horizon Monitor для социокультурного анализа и анализа настроений в соцсетях[4].

– Анализ поведения: Horizon Monitor отслеживает поведенческие паттерны, создавая уведомления на основе заданных критериев. Пример: компания настроила Horizon Monitor для выявления опасного поведения в социальных сетях[5].

– Социальное моделирование и прогнозирование: Horizon Monitor использует анализ данных для прогнозирования угроз, таких как беспорядки или насилие. Пример: правоохранительные органы применяют Horizon Monitor для

---

[1] shadowdragon.io
[2] johnhartley.org/wp-content/uploads/2021/10/ShadowDragon-might-be-the-social-media-surveillance-software-that-can-watch-your-every-move.pdf
[3] main.gerki.in/threads/103762/
[4] frost.com/wp-content/uploads/2024/02/ShadowDragon-Award-Write-Up.pdf
[5] assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-14/documents/702997/729871546736421-service-definition-document-2025-02-17-1634.pdf

выявления признаков беспорядков до их начала, основываясь на активности в соцсетях[1].

[1] theintercept.com/2021/09/21/surveillance-social-media-police-microsoft-shadowdragon-kaseware/

Список используемых источников

1. abc.xyz
2. academia.edu/121337437/The_DARPA_SocialSim_Challenge_Massive_Multi_Agent_Simulations_of_the_Github_Ecosystem
3. adesso.de/en/news/blog/cyber-kill-chain.jsp
4. adobe.com
5. adweek.com/programmatic/why-oracle-advertising-is-really-shutting-down/
6. aimresearch.co/market-industry/from-seaplanes-to-ai-how-lockheed-martin-transformed-defense-and-aerospace
7. aistrata.tech/mclasses/tpost/eedtnzmzv1-marketing-po-novomu-vliyanie-chatgpt-na
8. all-about-security.de/unveiling-liminal-panda-a-closer-look-at-chinas-cyber-threats-to-the-telecom-sector/
9. amazon.com
10. amentum.com
11. amentum.com/markets/intelligence/
12. amentum.com/our-capabilities/data-analytics-and-cyber/
13. amentum.com/our-capabilities/data-analytics-and-cyber/counter-intelligence-solutions/
14. amnesty.org.nz/palantir-technologies-contracts-raise-human-rights-concerns-nyse-direct-listing/
15. analytikaplus.ru/kak-snowflake-pomogaet-brendam-personalizirovat-kontent-dlya-millionov-klientov/
16. appercase.ru/news/5457/
17. appercase.ru/news/9532/
18. asdnews.com/news/defense/2023/05/03/kratos-takes-multimission-satellite-ground-system-support-demo-road
19. assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-14/documents/702997/729871546736421-service-definition-document-2025-02-17-1634.pdf
20. atlan.com/know/snowflake/snowflake-cortex-use-cases/
21. blog.hootsuite.com/twitter-algorithm/
22. blogs.lse.ac.uk/polis/2018/10/27/2018-brazil-elections-the-power-of-social-media-and-the-threat-to-journalism/
23. bloomberg.com/news/articles/2024-01-12/palantir-israel-agree-to-strategic-partnership-for-battle-tech
24. bloomberg.com/politics/articles/2018-05-16/microsoft-wins-lucrative-cloud-deal-with-intelligence-community
25. brandwatch.com/blog/marketing-brand-sustainability-effectively/
26. brandwatch.com/blog/social-media-monitoring/
27. business.adobe.com/products/adobe-analytics.html

28. campaigninginfo.com/how-to-use-linkedin-for-political-campaigns/
29. cision.com
30. cision.nl/en/prnewswire/
31. clearview.ai
32. cnbc.com/2021/03/29/amazons-pr-campaign-ahead-of-union-vote-shows-how-worried-it-is.html
33. compositepanel.ru/news/detail/tendentsii-razvitiya-rynka-30-03-2025-14-46-04/
34. crossdevicemediagroup.com/audience-targeting-with-trade-desk/
35. crowdstrike.com
36. currenttime.tv/a/video-kak-rabotayut-boty-v-sotssetyah/30200604.html
37. cyberscoop.com/chinese-disinformation-recorded-future/
38. d11jmx241r4rky.cloudfront.net/a/open-ai-rossiya-seti-vliyaniya/32973869.html
39. dailymail.co.uk/sciencetech/article-4889092/Amazon-authorized-host-DoD-s-sensitive-data.html
40. darpa.mil/news-events/2022-05-04a
41. darpa.mil/program/artificial-social-intelligence-for-successful-teams
42. darpa.mil/program/computational-cultural-understanding
43. darpa.mil/program/ground-truth
44. darpa.mil/program/influence-campaign-awareness-and-sensemaking
45. darpa.mil/program/semantic-forensics
46. darpa.mil/work-with-us/information-innovation-office
47. datacenterdynamics.com/en/analysis/enlisting-watson-ibm-on-winning-us-army-private-cloud-contracts/
48. datafloq.com/read/big-data-startup-review-recorded-future/
49. deepnewz.com/china/openai-bans-chinese-sneer-review-operation-using-chatgpt-influence-campaigns-1e14008e
50. designdevelopmenttoday.com/industries/aerospace/news/22943995/northrop-grumman-unveils-autonomous-testbed-ecosystem
51. deswalsh.com/2012/04/25/testing-the-social-media-engagement-management-tool-sprout-social-part-2/
52. developer.x.com/en/docs/x-api
53. diversedaily.com/command-and-control-simulation-understanding-algorithms-for-war-simulations/
54. d-russia.ru/tag/palantir
55. dzen.ru/a/Z6sECzanbRLqUA7o
56. en.wikipedia.org/wiki/PalantirTechnologies
57. en.wikipedia.org/wiki/Raytheon
58. epicos.com/article/880407/northrop-grummans-deep-sensing-and-targeting-technology-goes-airborne-advance-vision
59. ethans.co.in/blogs/elevate-your-marketing-strategy-with-salesforce/
60. fastercapital.com/ru/content/Ultimate-FAQ--Brandwatch--что--как--почему--когда.html

61. fedscoop.com/cia-quietly-awards-billion-dollar-c2e-cloud-contract/
62. fictionhorizon.com/deadpool-wolverine-dominates-nielsens-streaming-chart-in-its-disney-debut-week/
63. firebearstudio.com/blog/adobe-experience-cloud.html
64. forbes.com/sites/michaelposner/2019/09/12/what-companies-can-learn-from-palantir/
65. forbes.com/sites/stephenpastis/2024/10/07/could-republican-ties-to-x-impact-voters-heres-what-experts-say-as-trump-outspends-harris-on-the-site/
66. forbes.ru/reklama/298629-ibm-marketing-cloud-oblachnyi-otvet-na-zaprosy-rynka
67. fragrancelounge-ea.com/blog/sprinklr-insights-real-time-insights-social/?v=518f4a738816
68. frost.com/wp-content/uploads/2024/02/ShadowDragon-Award-Write-Up.pdf
69. ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance
70. gd.com
71. gdmissionsystems.com/cyber
72. graniteshares.com/institutional/us/en-us/research/what-does-palantir-technologies-do
73. habr.com/ru/companies/muk/articles/325330/
74. habr.com/ru/news/786422/
75. huffpost.com/entry/remote-neural-monitoring-used-in-unethical-army-psyop_b_587fe170e4b0fb40bf6c462a
76. ibm.com
77. idstch.com/technology/ict/artificial-social-intelligence-for-successful-teams-asist-pioneering-human-machine-collaboration/
78. idstch.com/technology/ict/darpa-ccu-developing-ai-enabled-automated-cultural-interpreters-and-dialogue-assistants/
79. idstch.com/technology/ict/darpa-next-generation-social-science-program-seek-new-models-theories-tools-predictive-science-social-phenomena/
80. idstch.com/technology/ict/darpa-socialsim-developing-effective-information-warfare-analysis-tools-for-social-media/
81. idstch.com/technology/ict/darpa-using-mind-control-techniques-manipulate-social-media/
82. insights.sei.cmu.edu/library/darpas-sematic-forensics-semafor-research-program/
83. investing.com/news/stock-market-news/oracle-reaches-115-million-consumer-privacy-settlement-3527333
84. itrportal.com/articles/2024/06/25/sprinklr-named-a-leader-in-digital-customer-interaction-solutions-report/
85. johnhartley.org/wp-content/uploads/2021/10/ShadowDragon-might-be-the-social-media-surveillance-software-that-can-watch-your-every-move.pdf

86. keepersecurity.com/blog/ru/2024/09/13/the-most-recent-credential-stuffing-attacks-on-companies-in-2024/
87. kratoscyber.com/
88. kratosdefense.com
89. leidos.com
90. leidos.com/markets/aviation/security-detection
91. leidos.com/products
92. leidos.com/sites/leidos/files/2023-02/Leidos-Zero-Trust%20Pentagon-DD.pdf
93. lockheedmartin.com
94. lockheedmartin.com/en-us/products/integrated-intelligence-surveillance-reconnaissance-systems.html
95. main.gerki.in/threads/103762/
96. meta.com
97. microsoft.com
98. nap.nationalacademies.org/read/25271/chapter/12
99. nbcnews.com/tech/internet/republican-bot-campaign-trump-x-twitter-elon-musk-fake-accounts-rcna173692
100. news.adobe.com/news/news-details/2022/adobe-to-help-u-s-bank-accelerate-personalization-in-consumer-banking
101. nielsen.com
102. nielsen.com/solutions/media-planning/audience-segments/
103. nielsen.com/solutions/scarborough
104. northropgrumman.com
105. npr.org/2025/06/05/nx-s1-5423607/openai-china-influence-operations
106. nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html
107. nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html
108. nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html
109. nytimes.com/2019/10/25/technology/dod-jedi-contract.html
110. nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html?ysclid=mcbsazt6rv719969351
111. nytimes.com/2025/05/30/technology/trump-palantir-data-americans.html
112. nytimes.com/interactive/2019/06/08/technology/youtube-radical.html
113. nytimes.com/interactive/2020/10/21/magazine/palantir-alex-karp.html?ysclid=mc7pzcm92k679859992
114. okocrm.com/blog/zachem-prognozirovat-povedenie-klientov/
115. openai.com
116. openaisuite.com/predictive-analytics-forecasting-the-future-with-big-data/
117. oracle.com
118. palantir.com/impact/world-food-programme/
119. palantir.com/offerings/intelligence/
120. palantir.com/palantir-is-not-a-data-company/

121. palantir.com/partnerships/aws/
122. palantir.com/platforms/aip/
123. palantir.com/platforms/foundry/
124. palantir.com/uk/healthcare/
125. prodelo.biz/uslugi-opencart/stsenarii-avtomatizatsii/n8n/analiz-postov-na-reddit-s-pomoschyu-ii-dlya-poiska-biznes-vozmozhnostey
126. raytheon.co.uk/what-we-do/cyber-space-and-training/mission-intelligence
127. recordedfuture.com
128. redwerk.com/blog/microsoft-azure-cognitive-services/
129. reuters.com/article/us-usa-election-google-idUSKCN1ML1WJ
130. reuters.com/business/palantir-raises-annual-revenue-forecast-booming-ai-demand-2025-05-05/
131. rittmanmead.com/blog/2017/02/analysing-elections-data-with-oracle-data-visualisation-desktop/
132. rolustech.com/blog/content-strategy-salesforce-marketing-cloud
133. rtx.com
134. salesforce.com
135. salespanel.io/resources/b2b-linkedin-ads/
136. sdelaem.agency/blog/tendenczii-v-kontent-marketinge-v-2024-issledovanie-sprout-social/
137. shadowdragon.io
138. slaesforce-faq.com/do-political-campaign-s-use-salesforce
139. snowflake.com
140. snowflake.com/en/the-modern-marketing-data-stack-report/
141. sociable.co/social-media/darpa-to-exploit-social-media-messaging-blog-data-to-track-geopolitical-influence-campaigns/
142. sociable.co/technology/darpa-ai-moderate-social-media-groups-destructive-ideas-humanitarian-efforts/
143. sociable.co/technology/local-mentality-darpa-program-has-non-military-potential-for-learning-about-different-cultures/
144. spaceotechnologies.com/blog/how-to-use-openai-for-business-data-analysis/
145. sprinklr.com
146. sprinklr.com/stories/luxury-car-company/
147. sproutsocial.com
148. sproutsocial.com/insights/case-studies/pennstatehealth/
149. sproutsocial.com/insights/social-media-monitoring/
150. strangesounds.org/2022/05/darpa-wants-to-model-how-disinformation-flows-from-fringe-to-mainstream-platforms.html
151. supplychaintoday.com/palantir-technologies-cheat-sheet/
152. survey.money/blog/national-consumer-panel-review/
153. techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/

154. techgolly.com/palantir-and-the-role-of-big-data-in-government-surveillance
155. theguardian.com/technology/2025/jan/17/eu-asks-x-for-internal-documents-about-algorithms-as-it-steps-up-investigation
156. theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
157. theintercept.com/2021/09/21/surveillance-social-media-police-microsoft-shadowdragon-kaseware/
158. thetechherald.com/articles/Data-intelligence-firms-proposed-a-systematic-attack-against-WikiLeaks/12751/
159. thetimes.co.uk/article/ukraine-is-outflanking-russia-with-ammunition-from-big-tech-lxp6sv3qz
160. thetradedesk.com
161. thetradedesk.com/uk/our-demand-side-platform
162. time.com/6691662/ai-ukraine-war-palantir/
163. translated.turbopages.org/proxy_u/en-ru.ru.325c09eb-685bd002-d2945693-74722d776562/https/ultimatepopculture.fandom.com/wiki/Nielsen_ratings
164. translated.turbopages.org/proxy_u/en-ru.ru.f558ddf9-685bae2c-ace9b101-74722d776562/https/tutorialspoint.com/salesforce-integration-with-social-media-maximizing-your-reach
165. truth11.com/semantic-forensics-semafor-darpas-new-mass-surveillance-disinformation-control-tool/
166. vc.ru/telegram/1675482-zabud-o-kastdevah-i-nachni-analizirovat-svoyu-auditoriyu-pri-pomoshi-chat-gpt-dazhe-esli-net-bloga
167. washingtonpost.com/technology/2020/06/10/amazon-rekognition-police/
168. washingtonpost.com/technology/2020/11/01/facebook-election-misinformation/
169. washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/
170. web.archive.org/web/20080417031944/http://findarticles.com/p/articles/mi_m0IBS/is_3_26/ai_67544226
171. web.archive.org/web/20230321051530/northropgrumman.com/cyber/
172. wfp.org/news/palantir-and-wfp-partner-help-transform-global-humanitarian-delivery
173. wired.com/story/palantirs-gods-eye-view-of-afghanistan/
174. wsj.com/articles/adobe-plans-to-ban-political-ads-on-its-online-ad-sales-platform-11596222336
175. x.com
176. xakep.ru/2018/07/12/military-docs-leak/
177. zdnet.com/article/raytheon-riot-defense-spying-is-coming-to-social-networks/