

Искусственный интеллект как инструмент цифрового превосходства КНР в Web 4.0 и информационных войнах

Захарова Анна
Тришкина Валерия

Семинар в рамках НУГ «АСЕАН+, БРИКС+, НАТО+: перспективы
азиатской интеграции в новом мировом порядке»

Table of contents

01

Нормативно-правовое
регулирование и
стратегия развития
ИИ в Китае, **AI Arms
Race**

02

Инструменты
воздействия и
ведение кампаний в
условиях роста
киберсуверенитета



01

Китай в гонке AI

Что значит ИИ для геополитики сегодня?

1. ИИ = **технология стратегического значения (POWER)**: влияет на безопасность, экономику и цифровой суверенитет
2. Китай – не просто потребитель ИИ, а **активный регулятор и экспортер стандартов**
3. **Гипотеза**: поэтапное регулирование ИИ в Китае приведет к созданию единого законодательства, способного влиять на глобальные нормы, и лидерству Китая в **AI Arms Race**



Китайская цифровая стратегия: контекст

- Интеграция ИИ в программы государственного развития:
 - **«Сделано в Китае 2025»** — ставка на автономные технологии
 - **«План развития искусственного интеллекта нового поколения»**
(《新一代人工智能发展规划》, 2017 г — цель: лидерство к 2030)
 - **План Интернет+ и развитие Web 4.0** = полная интеграция ИИ, 6G, квантовой связи и IoT
- **ИИ** — часть цифрового суверенитета и «архитектуры власти»

Этапы регулирования ИИ в КНР



2016–2020

Стратегии +
саморегулирование
бизнеса



2021

Сформулированы
все законы о
персональных
данных (PIPL), о
безопасности
данных



2022–2023

Переход к обязательным
мерам:

- Регулирование рекомендательных алгоритмов и данных
- Контроль deepfake и синтетических медиа
- Права и обязанности генеративных ИИ (ChatGPT-аналоги: DeepSeek, X-GPT)

Законодательная иерархия

Национальные
планы,
конвенции и
стратегии
развития ИИ

«План развития искусственного интеллекта нового поколения 2017», Интернет+, Белая книга больших данных, «Сделано в Китае – 2025», «План развития индустрии больших данных», «13-й пятилетний план социально-экономического развития КНР (2016–2020)» и др.

Основные законы,
регулирующие
применение и аудит
безопасности данных

Закон о защите персональной информации (中华人民共和国个人信息保护法, **PIPL**), Закон о безопасности данных (中华人民共和国数据安全法 **Data Security**)

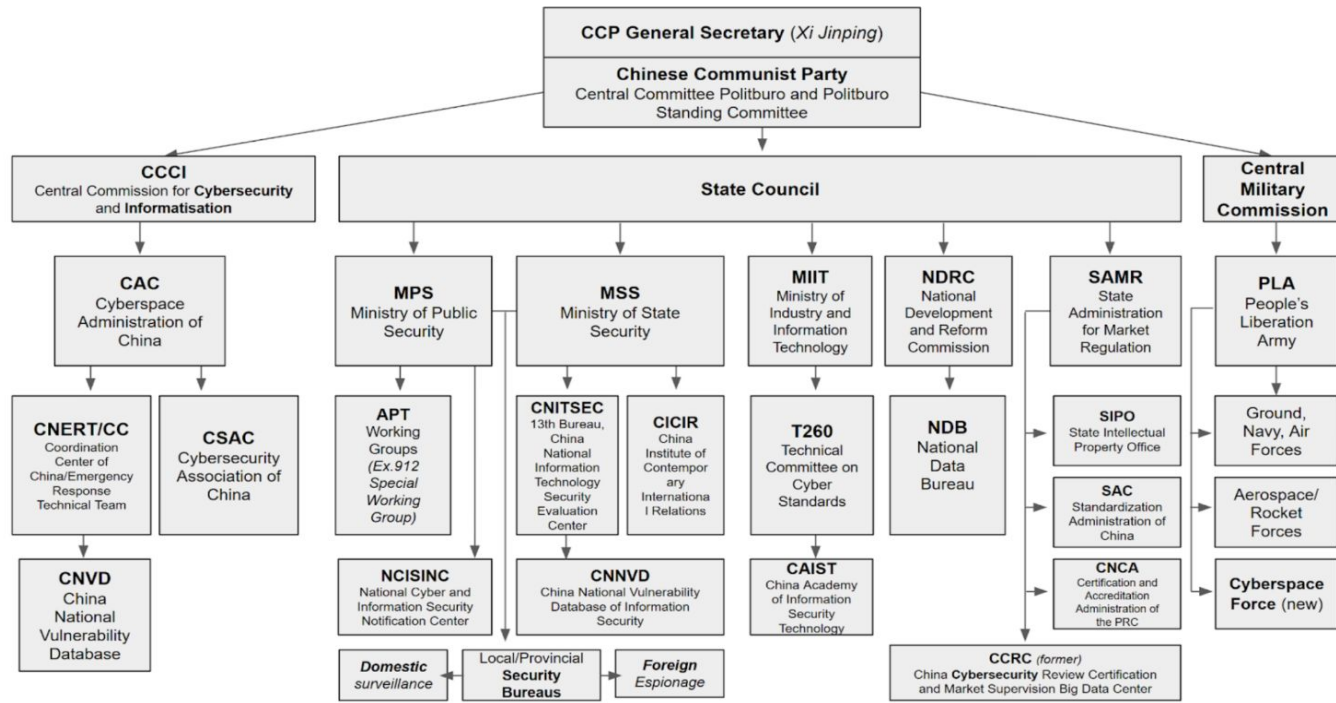
Распоряжения (guidelines),
локальные акты и положения,
регулирующие деятельность
бизнеса, операторов сотовой
связи и риск-менеджмент при
использовании ИИ

«Основные требования безопасности к услугам генеративного ИИ» (ТС260-003), «Положения об управлении алгоритмическими рекомендациями в интернет-сервисах», «Меры по управлению услугами генеративного искусственного интеллекта» и т.д.

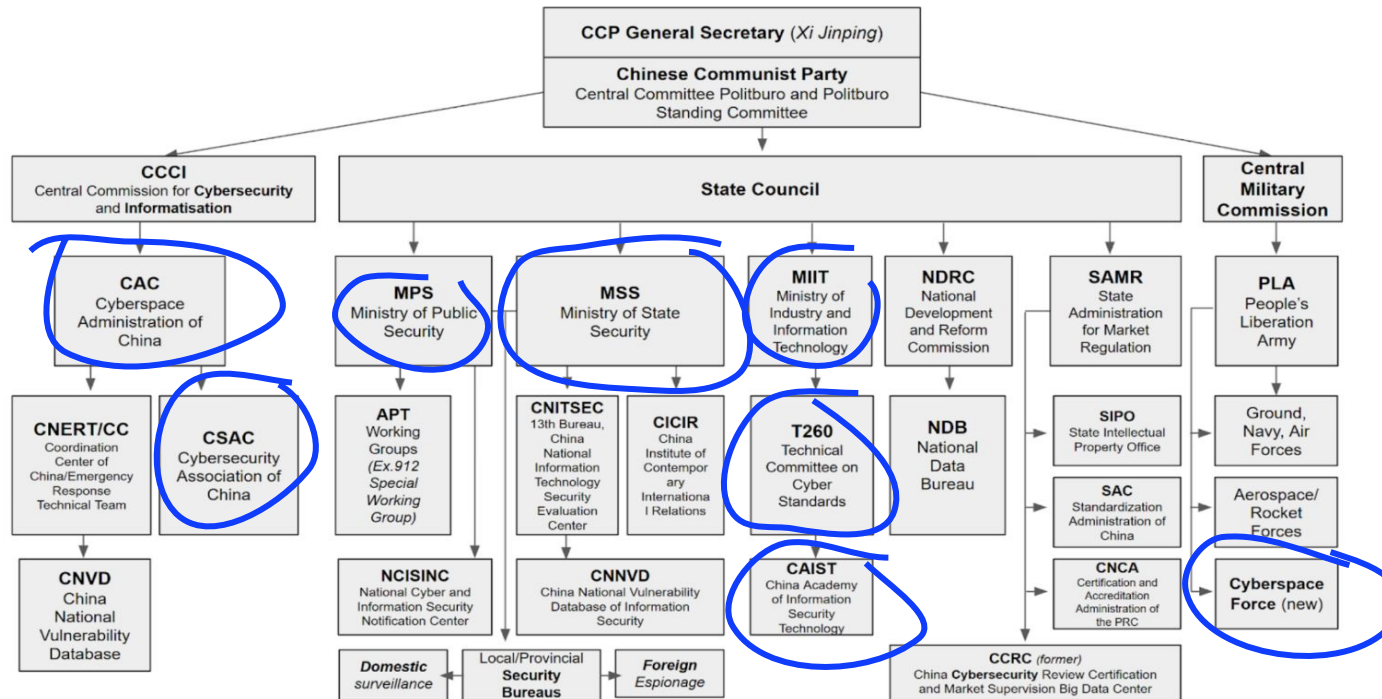
Примеры “точечных” законов и распоряжений

- «Положения об управлении алгоритмическими рекомендациями в интернет-сервисах» (互联网信息服务算法推荐管理规定, 2021 г.; вступили в силу 1 марта 2022 года);
- «Положения об управлении технологиями глубокой генерации в интернет-сервисах» (互联网信息服务深度合成管理规定, 2022 г.; вступили в силу 1 января 2023 года);
- «Меры по управлению услугами генеративного искусственного интеллекта» (生成式人工智能服务管理办法, 2023 г.; вступили в силу 15 августа 2023 года)

Кто регулирует ИИ в Китае?



Кто регулирует ИИ в Китае?



Кто регулирует ИИ в Китае?

- **CAC** – главный орган по контролю онлайн-сервисов и алгоритмов (Администрация киберпространства)
- **MIIT** – отвечает за промышленное внедрение ИИ (промышленность и информатизация)
- **MPS** – общественная безопасность, видеонаблюдение, «Золотой щит»
- **MOST** – формирует научные и этические стандарты (наука и технологии)
- **TC260/TC28** – технические комитеты: стандарты ИИ и кибербезопасности (рабочие органы)



Орган

Полное название (кит.)

Функции

Документы / инициативы

Государственный совет КНР

国务院

Координация стратегий
развития

Общая координация
«Плана развития ИИ
нового поколения»

Министерство науки и
технологий (MOST)

科技部 / 中华人民共和国科学技术部

Научно-техническая
политика,
финансирование, этика
ИИ

Руководство
Консультативного
комитета и Офиса по ИИ

Министерство
промышленности и
информатизации (MIIT)

工业和信息化部

Промышленное
развитие, поддержка ИТ,
внедрение ИИ

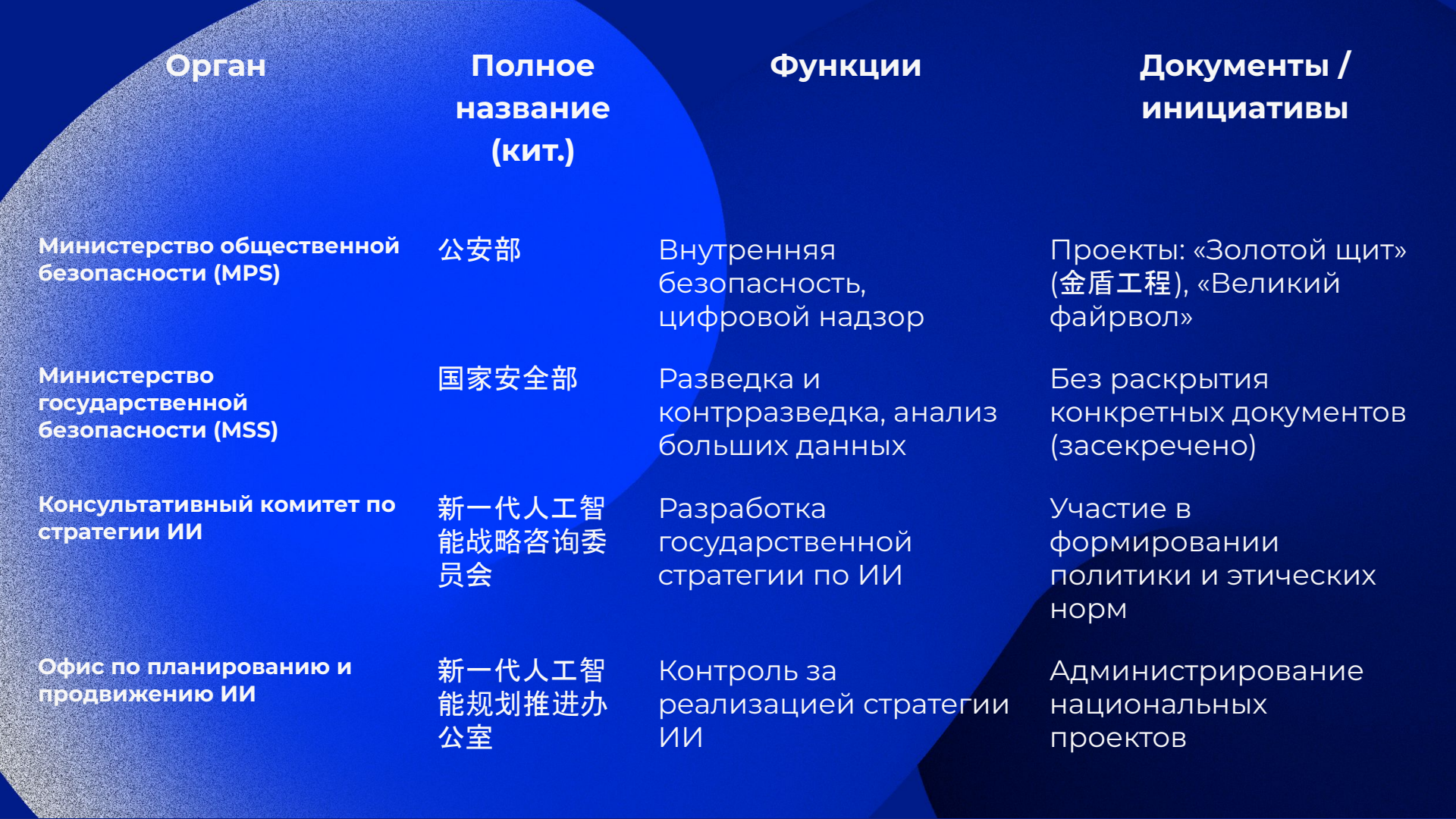
Трёхлетний план
развития ИИ-индустрии
(2018–2020)

Администрация
киберпространства Китая
(CAC)

国家互联网信息办公室

Надзор за интернет-
контентом,
регулирование ИИ в
онлайн-среде

Совместные
нормативные акты по
генеративному ИИ



Орган

Полное название (кит.)

Функции

Документы / инициативы

Министерство общественной безопасности (MPS)

公安部

Внутренняя
безопасность,
цифровой надзор

Проекты: «Золотой щит»
(金盾工程), «Великий
файрвол»

Министерство
государственной
безопасности (MSS)

国家安全部

Разведка и
контрразведка, анализ
больших данных

Без раскрытия
конкретных документов
(засекречено)

Консультативный комитет по
стратегии ИИ

新一代人工智能
战略咨询委员会

Разработка
государственной
стратегии по ИИ

Участие в
формировании
политики и этических
норм

Офис по планированию и
продвижению ИИ

新一代人工智能
规划推进办公室

Контроль за
реализацией стратегии
ИИ

Администрирование
национальных
проектов

ИИ и цифровой контроль внутри страны, Министерство общественной безопасности (MPS) 公安部

«Золотой щит»

видеонаблюдение,
биометрия,
предиктивная
аналитика

«Великий файрвол»

блокировка
контента, DPI,
цензура

MLPS 2.0

классификация
ИТ-систем, защита
нацданных

Ключевые принципы законодательного регулирования ИИ в Китае

- 1. Модерация контента**
- 2. Защита персональных данных**
- 3. Алгоритмическое управление (Безопасность, Этика, Прозрачность)**
- 4. Проактивное применение в системах контроля и фильтрации (MLPS 2.0, Great Firewall, Golden Shield)**

Саморегулирование ИИ в науке и индустриализации

Научные и исследовательские учреждения

Китайская академия наук (CAS, 中国科学院)

— проводит исследования в области ИИ (например, Институт автоматизации CAS).

Пекинская академия искусственного интеллекта (北京智源人工智能研究院)

— государственно-частная структура, фокусирующаяся на передовых разработках ИИ.

Общество искусственного интеллекта Китая (CAAI, 中国人工智能学会)

— объединяет экспертов, участвует в выработке технических и этических стандартов.

Отраслевые и саморегулируемые объединения

Шэньчжэньская ассоциация индустрии искусственного интеллекта (深圳市人工智能行业协会)

— разработала отраслевую конвенцию по этике и саморегулированию ИИ.

Альянс индустрии искусственного интеллекта (人工智能产业联盟)

— участвует в формировании правил и стандартов этического применения ИИ.

**Национальные
стратегии развития
(экономика, патенты, в
т.ч. военная
индустрия)**

AI

**= комплексная
национальная
мощь (综合国力)**

**Динамическая
законодательная база
и разветвленный
административный
аппарат**

**Наука и
технологии**



Международная экспансия модели контроля развития ИИ в КНР

- **Экспорт технологий ИИ:** Huawei, ZTE, Hikvision — Африка, Азия, Латинская Америка
- **«Цифровой Шёлковый путь»:** инфраструктура + зависимости от стандартов КНР
- **Принцип киберсуверенитета** — продвигается в ООН, ITU
- Китай предлагает другим странам не просто оборудование, а модель цифрового управления (концепция: **Пекинский консенсус**)

Китайский vs Западный подход к ИИ продукту

	DeepSeek (Китай)	ChatGPT (США)
Исходный код	Открытый	Закрытый
Владение	Китайский стартап, поддержка от госструктур	Частная компания (OpenAI, Microsoft)
Цели	Независимость, продвижение стандартов КНР	Коммерциализация, глобальный рынок
Регуляция	Централизованное, сертификация САС	Саморегулирование + общие нормы
Прозрачность	Обязательная маркировка, аудит, есть политическая цензура	Частичная, зависящая от компании, цензура касающаяся общих вопросов этики

КНР vs Запад

- Регулирование сверху, цензура, контроль
- Государственный приоритет над свободой слова, упор на **развитие государственности и безопасности в интернете**
- ИИ = элемент политической стабильности и **суверенитета**

- Права пользователя, открытость, этика ИИ
- Deep State скрыт от конечного пользователя
- Саморегулирование, мультистейкхолдерность, доминирование корпораций
- ИИ = сервис и инновация для **потребителя**

01 - Выводы

- Китай системно строит архитектуру цифрового контроля через ИИ
- Постепенное регулирование выливается в экосистему глобального значения
- В Web 4.0 Китай претендует быть не просто участником, а **нормотворцем**
- ИИ сегодня — это не только технология, но и инструмент власти, стандартов и суверенитета



02

Китай и информационные войны

Информационные войны. Взгляд

Термин (кит.)	Транскрипция	Перевод	Основной акцент	Особенности	Контекст и функции в дискурсе
信息战	xìnxī zhàn	Информационная война	Техническая сторона, высокие технологии	Электронные операции, кибератаки, системы защиты, разведка	Подчеркивает технологический и военный аспект
舆论战	yúlùn zhàn	Война общественного мнения	Идеологическое противостояние	Манипуляция нарративами, влияние на массовое сознание	Формирование общественной установки и идеологии

Терминология

Термин (кит.)	Транскрипция	Перевод	Основной акцент	Особенности	Контекст и функции в дискурсе
资讯战	zīxùn zhàn	Информационная война (широкая)	Широкий спектр информационных потоков	Используется в традиционной письменности (Тайвань, Гонконг)	Фокус на разнообразии информации и коммуникациях
媒体战	méitǐ zhàn	Медийная война	Контроль каналов и платформ распространения	Влияние на доступ к информации и настроение аудиторий	Война за медийное пространство и информационные ресурсы

**Белая книга «Военная
стратегия Китая» (май
2015)**



*«Использовать информационные
системы для интеграции
различных боевых сил, боевых
подразделений и боевых
элементов в единую
боеготовность, чтобы
соответствовать основным
требованиям противостояния
в условиях информационной
войны.»*

Речь Си Цзиньпина на форумах по кибербезопасности и информатизации



*«Космос и киберпространство стали новыми командными высотами для стратегической конкуренции между всеми сторонами». «Мы должны занять глобальную позицию, систематически и проактивно планировать развитие **искусственного интеллекта** на национальном стратегическом уровне и твердо взять в свои руки стратегическую инициативу в международной конкуренции на новом этапе развития искусственного интеллекта».*



План развития ИИ нового поколения (июль 2017)

«Активно развивая искусственный интеллект, мы должны придавать большое значение возможным рискам и проблемам безопасности, усиливать дальновидные меры профилактики и сдерживания, минимизировать риски и обеспечивать безопасное, надежное и контролируемое развитие искусственного интеллекта».

Инструментарий КНР в инфовойнах



Умаодан

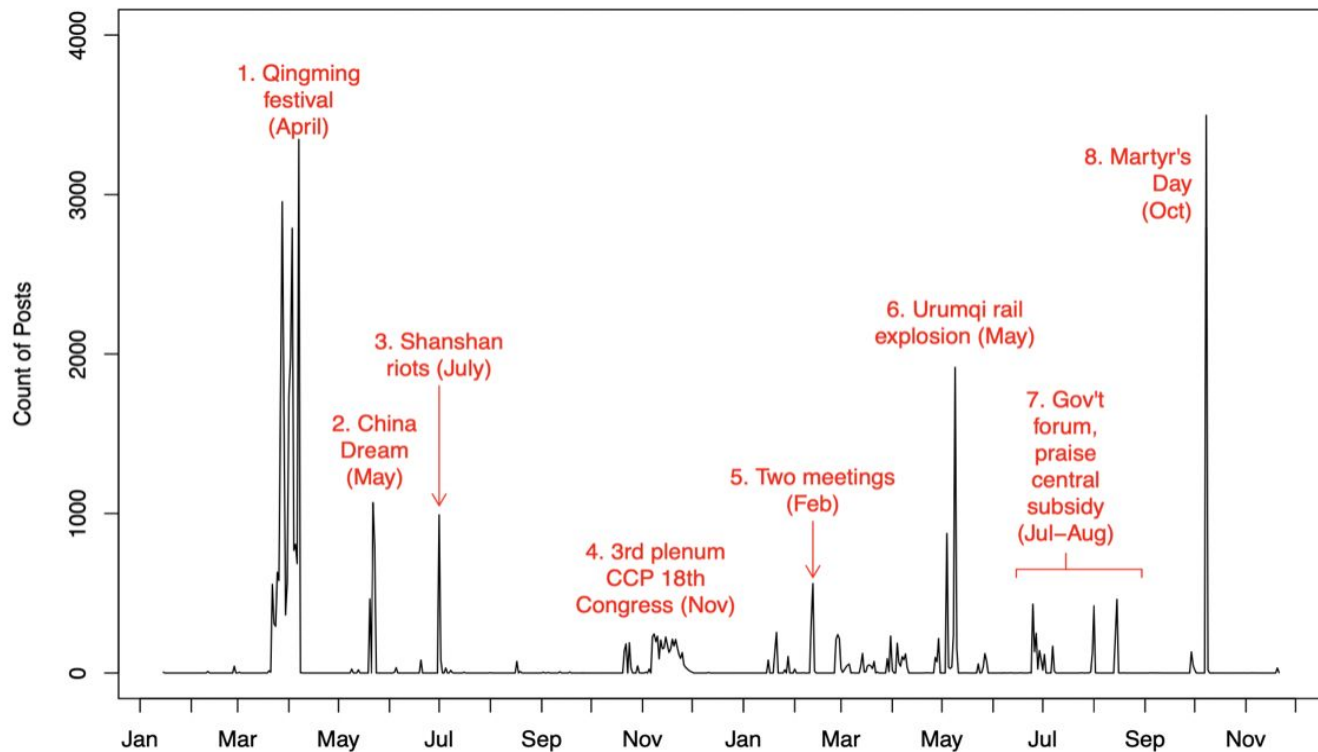


Цзыганью

Умаодан

- В Китае действуют проправительственные комментаторы «Умаодан» («50 центов»), которые работают на онлайн-платформах.
- Их задача — быстро реагировать на критику и создавать позитивный имидж власти.
- Государство ограничивает протесты, создавая «зону относительной свободы» в интернете.
- «Умаодан» — это сотрудники и лояльные добровольцы с множеством фейковых аккаунтов.
- Они не вступают в дебаты, а публикуют позитивные и отвлекающие сообщения.

Умаодан



Цзыганьу

- 自干五 — это добровольные проправительственные комментаторы в Китае, не получающие официальных вознаграждений.
- Обычно это патриотично настроенные граждане, активно защищающие политику КПК в интернете.
- В отличие от «Умаодан», 自干五 действуют спонтанно и без строгой координации.



Искусственный интеллект как инструмент информационных войн КНР

- Китайские ИИ-боты способны генерировать и распространять до 45% всех сообщений в ключевых социальных сетях, контролируемых государственными структурами
- в 2022 году КНР задействовала более 500 тысяч активных ИИ-ботов в глобальных информационных кампаниях, направленных на продвижение интересов страны в Юго-Восточной Азии, Африке и Латинской Америке.

Аналитика больших данных

Китайские структуры применяют алгоритмы машинного обучения для мониторинга и обработки огромных массивов информации, что позволяет:

- Выявлять и оперативно нейтрализовать критические информационные угрозы;
- Предсказывать поведенческие паттерны целевых аудиторий;
- Настраивать персонализированные воздействия, повышая эффективность психологических операций.

Спасибо за ВНИМАНИЕ!

Будем рады ответить на ваши вопросы

Захарова Анна
Тришкина Валерия

Семинар в рамках НУГ «АСЕАН+, БРИКС+, НАТО+:
перспективы азиатской интеграции в новом
мировом порядке»