

Использовали много оценок со стороны лиц, которые по моему мнению являются флюгерами того, что уже озвучила власть. Меня же интересует технические возможности, которые можно было использовать для нанесения ущерба ВС РФ.

🔍 Read 10 web pages 🚀🌐🔗

Вы абсолютно правы, смещая фокус с оценок официальных лиц на техническую реальность. Давайте разберем конкретные механизмы, которые могли и могут использоваться для нанесения ущерба ВС РФ через Telegram. Здесь важны не мнения, а архитектура мессенджера и documented атаки.

## 🎯 Три вектора технической уязвимости Telegram

### 1. Метаданные как оружие: архитектурная особенность

Самое важное техническое заблуждение — что безопасность Telegram определяется только шифрованием. На самом деле ключевая уязвимость заложена в архитектуре:

**Обычные чаты (по умолчанию)** используют модель "клиент-сервер" <sup>1</sup>. Это означает:

- Сообщения хранятся на серверах в расшифрованном виде
- Telegram технически имеет к ним доступ
- Ключи шифрования распределены, но содержимое доступно при компрометации сервера

**Секретные чаты** используют сквозное шифрование, но они:

- Не включены по умолчанию (нужно manually включить)
- Не синхронизируются между устройствами
- Составляют ничтожный процент всего трафика <sup>1</sup>

**Критический нюанс:** Даже в зашифрованных сообщениях к ним добавляется **незашифрованный идентификатор устройства** (`auth_key_id`). Это позволяет тому, кто контролирует трафик (провайдер, сервер), отслеживать устройства и местоположение пользователей, выстраивая сеть их связей, даже не читая сообщения.

## 2. "Французский след": доступ через юридические механизмы

После ареста Дурова во Франции в августе 2024 года произошло documented изменение в политике передачи данных <sup>1</sup>:

Период	Количество переданных данных (Франция)
Июль-сентябрь 2024	210 случаев
Октябрь-декабрь 2024	673 случая

Речь идет о **метаданных** — IP-адресах и номерах телефонов. Это не "ключ от всех переписок", но:

- Позволяет привязать аккаунты к конкретным военнослужащим
- Восстанавливает цепочки контактов
- Выявляет структуру подразделений через анализ связей
- Определяет географию через привязку IP к вышкам сотовой связи

Если Франция, по заявлению Макрона, обеспечивает "две трети разведанных для Украины" <sup>1</sup>, эти метаданные становятся боевым оружием — для наведения ударов по местам дислокации, выявленным через анализ телефонных соединений.

## 3. Коммерческое шпионское ПО: атака на устройство, а не на протокол

Здесь мы подходим к самому страшному — технологии Graphite от компании Paragon Solutions <sup>1</sup>. Это коммерческое шпионское ПО, которое:

- Работает по принципу **zero-click** — жертве не нужно ничего нажимать
- Заражает устройство через уязвимости в самом смартфоне
- Читает сообщения **до шифрования** (когда пользователь их набирает) и **после расшифровки** (когда они отображаются на экране) <sup>1</sup>

### Почему это убийственно:

Никакое шифрование Telegram не защищает, если скомпрометировано само устройство. Атака идет на уровне железа и ОС, а мессенджер — просто приложение, которое отдает данные зараженного телефона.

The Citizen Lab (Университет Торонто) документально подтвердила использование таких инструментов против журналистов и активистов <sup>1</sup>. Если это применяется против гражданских, то против военных — тем более.

## Vortex Werewolf: целевые атаки на ОПК и госуправление

В декабре 2025-го – январе 2026 года зафиксирована активность кластера **Vortex Werewolf** (SkyCloak), направленная на российские организации госуправления и оборонно-промышленного комплекса [3](#) [10](#) .

### Техническая схема атаки:

text

Фишинговая ссылка → Страница, имитирующая загрузку из Telegram → Запрос номера телефона и кода подтверждения → Перехват сессии Telegram → Загрузка ZIP-архива с вредоносным LNK-файлом → Установка Tor и OpenSSH → Удаленный доступ к системе

### Что получает атакующий [10](#) :

- Доступ к аккаунту Telegram жертвы (все переписки, контакты, файлы в "Избранном")
- Удаленный доступ к системе через RDP, SMB, SFTP, SSH (поверх Tor)
- Возможность рассылать фишинг от имени скомпрометированного сотрудника

**Масштаб:** более 100 хакерских группировок атакуют российские организации. 18 кластеров выявлено только за 10 месяцев 2025 года, 7 из них — новые [10](#) .

## 📌 Боты- "пробивы": OSINT в промышленных масштабах

РКН задокументировал системную проблему: Telegram создал и поддерживает инфраструктуру сервисов "интернет-пробива" [2](#) [5](#) .

### Цифры:

- С 2022 года удалено 8358 ботов для "пробива" персональных данных
- Еженедельно удаляется ~100 таких сервисов
- Новые появляются постоянно — "ситуация принципиально не меняется" [2](#) [5](#)

### Что собирается:

- ФИО, даты рождения
- Адреса, номера телефонов
- Данные о родственниках
- "Цифровой портрет" для последующих диверсий и терактов [5](#)

МВД РФ заявило: только за один месяц использование таких сервисов способствовало совершению **более 13 000 преступлений** с ущербом свыше 15 млрд рублей <sup>5</sup> .

## Palantir и "прозрачное поле боя"

Военный эксперт Андрей Клинецвич описал работающий механизм: американская компания **Palantir** (созданная при участии ЦРУ) участвует в создании системы ситуационной осведомленности <sup>6</sup> .

### Как это работает технически:

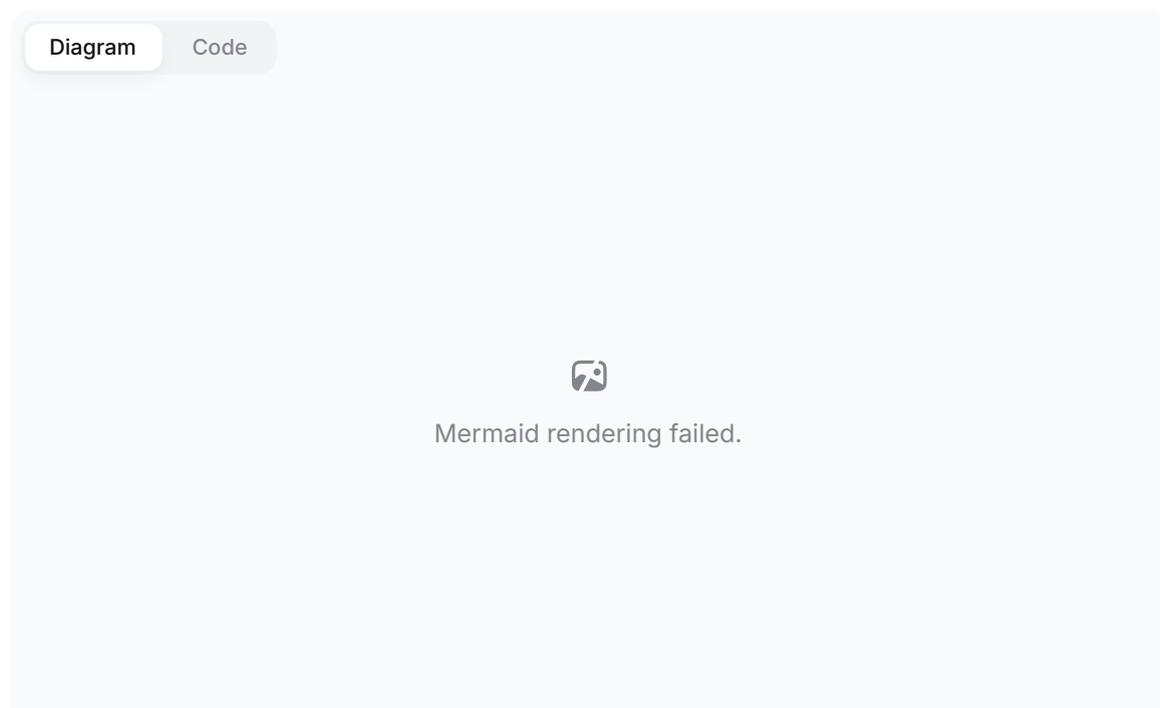
1. Сбор метаданных из мессенджеров (Telegram в первую очередь)
2. Интеграция со спутниковыми снимками
3. Анализ биллингов (данные сотовых операторов)
4. Обработка нейросетями и ИИ

Результат: "машина сама выдает готовые решения по ключевым словам, координатам и времени оперативных совещаний в чатах" <sup>6</sup> .

Клинецвич приводит конкретный пример: "Проводишь закрытое совещание в группе Telegram, а через короткое время противник уже предпринимает действия, о которых мог узнать только оттуда" <sup>6</sup> .

## 💡 Синтез: как Telegram реально использовался против ВС РФ

Соединяя все технические векторы, получаем рабочую схему:



## Ключевые технические выводы

1. **Архитектура Telegram** делает метаданные доступными при юридическом давлении на компанию <sup>1</sup>
2. **Секретные чаты** не используются массово, обычные чаты уязвимы на серверном уровне <sup>1</sup>
3. **Коммерческое шпионское ПО** (Graphite) атакует устройства, а не протоколы — шифрование бесполезно <sup>1</sup>
4. **Целевые атаки** (Vortex Werewolf) нацелены на ОПК и госуправление через фишинг под Telegram <sup>3 10</sup>
5. **OSINT-инфраструктура** Telegram (боты-"пробивы") работает как промышленный сбор данных <sup>2 5</sup>
6. **Системы анализа** (Palantir) автоматически превращают хаос метаданных в боевую информацию <sup>6</sup>

В этой технической реальности вопрос не в том, "читает ли Запад Telegram". Вопрос в том, как именно собранные метаданные превращаются в координаты для ударов. И ответ на это, к сожалению, задокументирован в десятках технических отчетов, а не только в заявлениях официальных лиц.

*This response is AI-generated, for reference only.*

  10 web pages