Meta's Q2 2023 Adversarial Threat Report

Domain Policy Recommendations
ICANN Hamburg Meeting - October 2023

Meta

Intellectual Property Enforcement &

Domain Policy Lead

Agenda

What is Coordinated Inauthentic Behavior (CIB)?

Examples of CIB from Q2 Report - Spamouflage and Doppelganger

Role of Domain Names in CIB attacks

How Meta tackles Domain Abuse at scale

Cross Community Recommendations

Q&A

Transparency is the key to tackling some of the biggest challenges we collectively face online. Meta's Transparency reports help our industry to learn from each other, improve our respective systems, and keep people safe across the internet.

What is Coordinated Inauthentic Behavior (CIB)?

CIB is coordinated efforts **to** **manipulate public debate for a strategic goal**, in which **fake accounts** are central to the operation.

Concerns:

Response to CIB requires collaboration and mitigation across many platforms & Internet infrastructure, at a level not seen today

Examples of Coordinated Inauthentic Behavior (CIB)

Spamouflage – *Largest known cross-platform covert influence operation in the world*

Example - Targeting Journalists

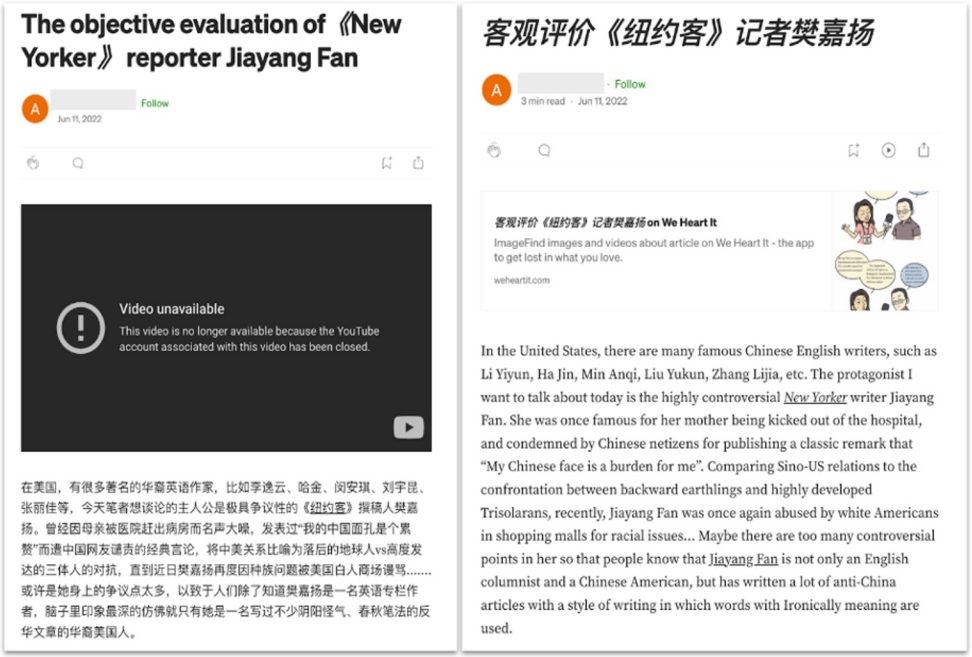
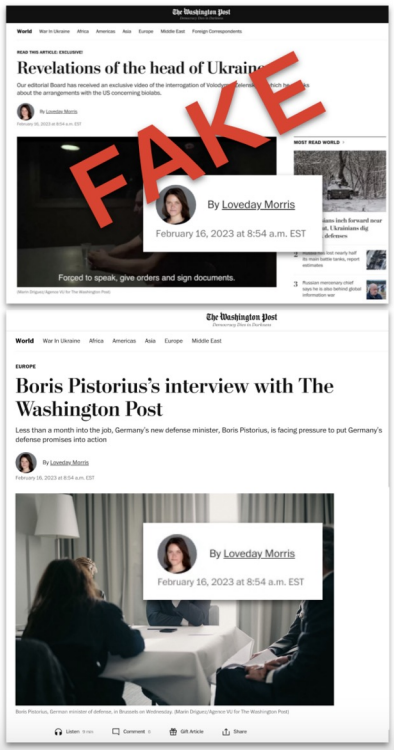


Image:

Two posts by the same Medium account, June 11, 2022. The English and Chinese versions are translations of one another, but with the headlines attached to the wrong texts.

Doppelganger – *largest & most aggressively persistent campaign disrupted in Russia since 2017*



Image

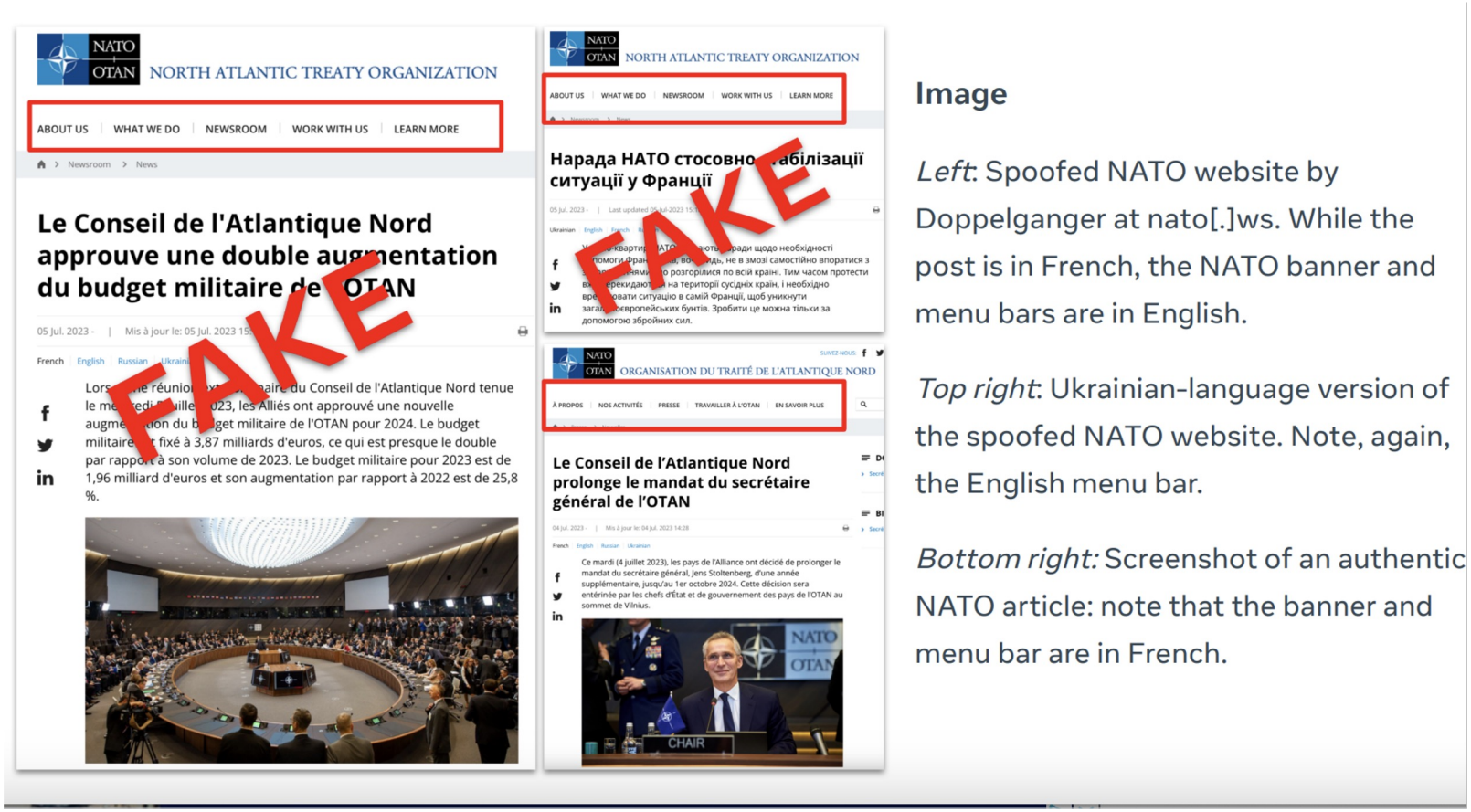
Top: Spoofed article by Doppelganger on washingtonpost[.]ltd purporting to show what appears to be a non-existent "interview" with Ukraine's President.

Top inset: Author name, profile picture and publication timestamp from the fake article.

Bottom: For comparison, an authentic article on the Washington Post website by the real author on the same day.

Bottom inset: Author name, profile picture and publication timestamp from the authentic article.

Doppelganger



Image

Left: Spoofed NATO website by Doppelganger at nato[.]ws. While the post is in French, the NATO banner and menu bars are in English.

Top right: Ukrainian-language version of the spoofed NATO website. Note, again, the English menu bar.

Bottom right: Screenshot of an authentic NATO article: note that the banner and menu bar are in French.

Role of Domain Names in CIB Attacks

4 out of 5
covert influence operations in the Meta Q2 2023 Report ran websites posing as independent news outlets

Our Approach to Countering Domain Abuse At Scale

Meta teams up with Anti-phishing and Brand Protection vendors to detect abuse

Address/remove harmful domains and URLs on Meta Platform

WHOIS Requests to Investigate and identify bad actors targeting our users

Mitigate off-platform abuse through Take-Down Requests, UDRPs or legal action

Establish Trusted Notifier Relationships for Swift Action

CHALLENGES IN MITIGATING CIB ATTACKS

WHOIS

- Domain Registrant unavailable
- Non-cooperating privacy or proxy service
- Contact data is inaccurate

LEGAL ACTION

UDRPs & Legal Action are too slow, expensive & unable to address the scale of abuse

DNS ABUSE

DNS abuse definitions, Voluntary frameworks, & ICANN contract amendments don't cover CIB

At Scale

- Reported & Removed 6,000+ abusive domain names targeting Meta Brands (2023)
- Mitigated 140,000 + phishing sites in 2022, a substantial decrease from prior year (265,000)
- WHOIS Reveals are only successful approximately 35% of the time, as reported by Tracer.ai

Our experience is not unique

Cross-Society Recommendations for Mitigating CIB

- Transparency and cross-society responses are key to tackling these malicious efforts to manipulate public debate

- Solutions are needed
  - @ICANN
  - Outside ICANN

Domain Specific Recommendations

@ICANN

- Improve ICANN contracts with Registrars (RRs)/Registries (RYs) to take proactive steps to address domain registration abuse ***at scale***
  - Require suspension of customer accounts for known bad actors
  - Impose additional verification for domain names that include a combination of famous brand plus words suggestive of fraud – like “login”, “password”, “security”, “help center”
  - Update the UDRP to disincentivize cybersquatting

Outside ICANN

- Adopt laws requiring complete, accurate, and verified WHOIS, similar to Europe’s Network and Information Systems Directive (NIS2):
  - RR and RYs to maintain complete & accurate WHOIS database, and follow best practices to verify information
  - RR and RYs to publish data of legal persons, & disclose data of natural persons on request to those with legitimate interests (e.g., to investigate & mitigate illegal activities)
- Incentivize cooperation with those investigating impersonating domain names and scams at scale
- Disincentivize cybersquatting by shifting costs from brand owners to abusive actors by enhancing the remedies or damages available under applicable law

Other Considerations

- Any such approach would need to account for legitimate criticism (such as BrandXsux[.]com), and be tailored to prevent powerful players from abusing them to silence lawful protest
- Encourage business and UN entities to adopt remedy and risk management approaches consistent with the UN Guiding Principles on Business and Human Rights

Let’s Talk!

For more information, read our blog on

Raising Online Defenses Through Transparency and Collaboration

&

Q2 2023 Adversarial Threat Report


Meta