BSIDES BUDAPEST

25MAY2023

A Deeper Look at the Disrupted Bot Farms in Ukraine

Anastasios Pingios

Disclaimer

All opinions expressed are my own, and do not represent my employer.

Introduction

Once upon a time...

5th Department
Political/internal security

└ 5th Service
Ideological counterintelligence

Russian Special Services

Russian Special Services

5th Service
Operational Information and International Relations Service
SCO's 4th Section, 16th Centre

6th Directorate
Electronic & Signals Intelligence

72nd Centre (GRITs)

Process

Identify tech savvy pro-Russian individuals

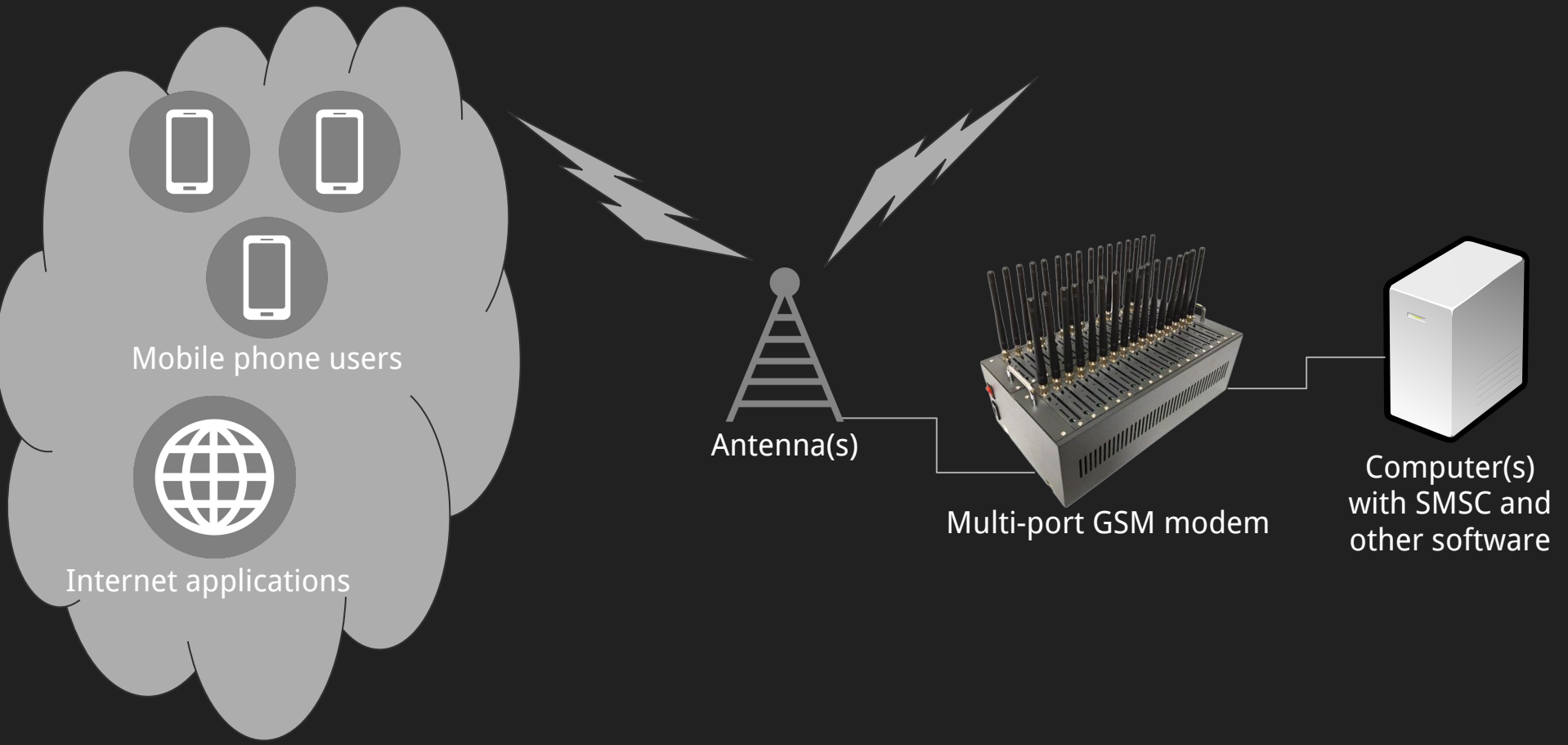
Recruitment & training

Payments (Russian platforms and cryptocurrencies)

Tasking

Operations

Architecture



Architecture

odem

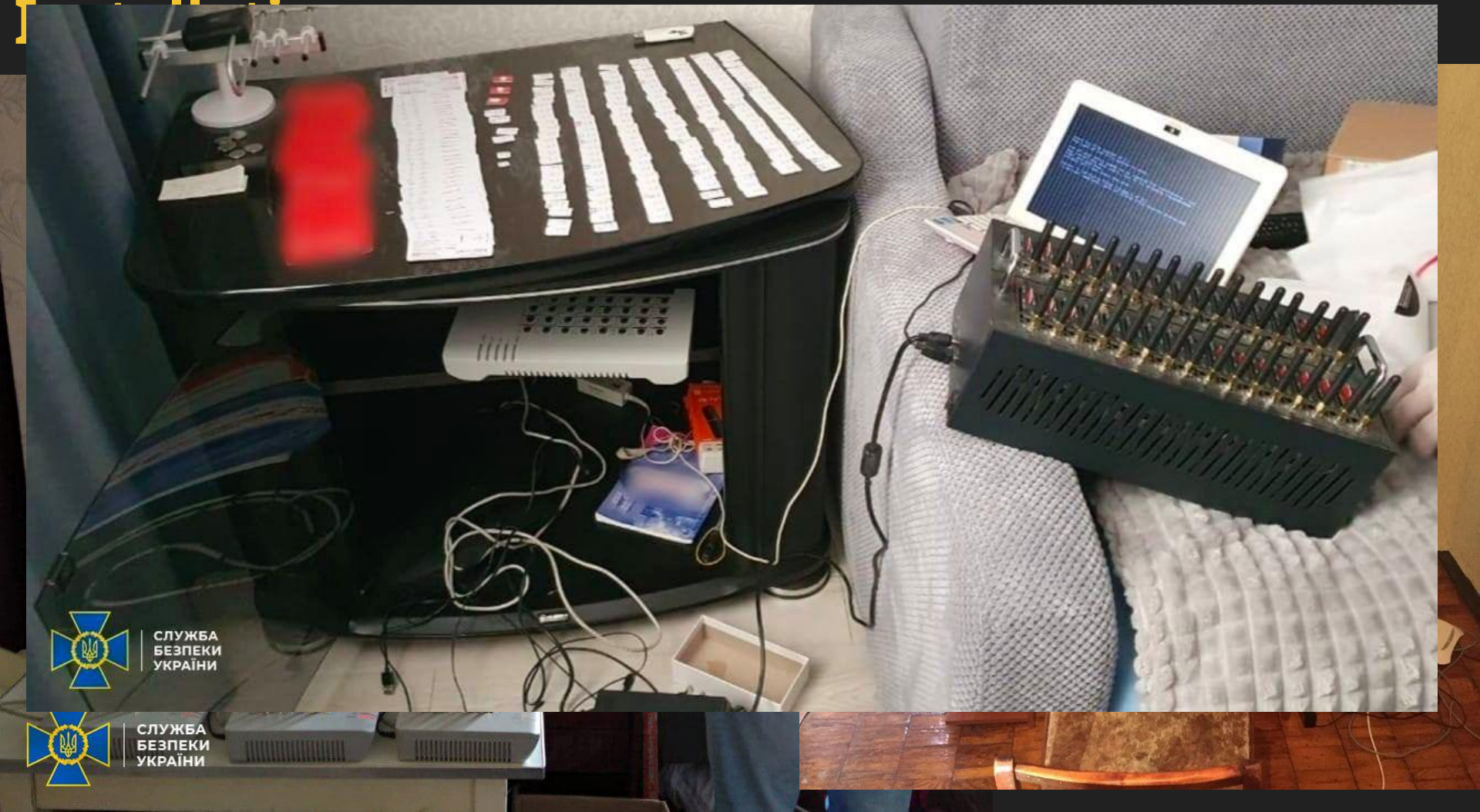
Computer(s) with SMSC and other software


СБУ
КІБЕРПОЛІЦІЯ
СБУ
СЛУЖБА
БЕЗПЕКИ
УКРАЇНИ


СЛУЖБА
БЕЗПЕКИ
УКРАЇНИ

Installations

Installations

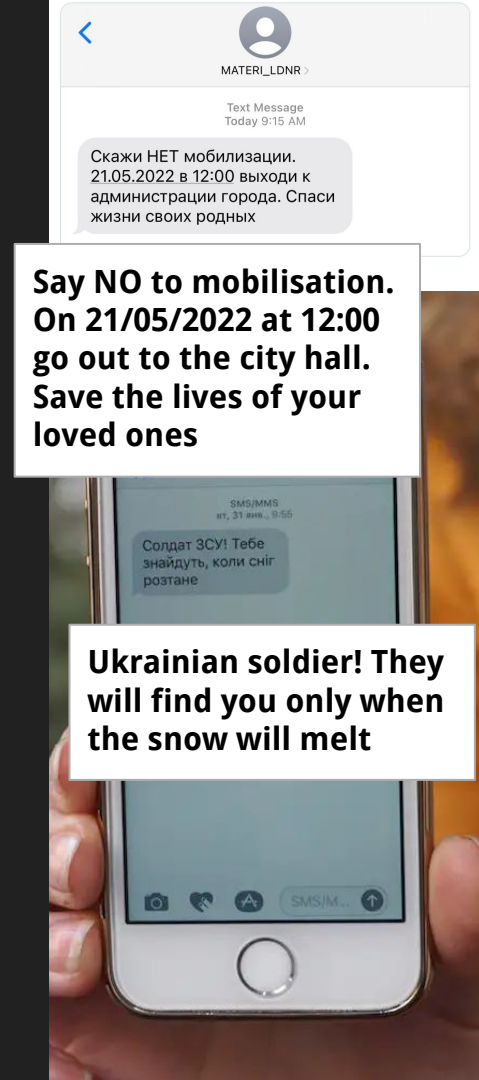

СЛУЖБА
БЕЗПЕКИ
УКРАЇНИ
СЛУЖБА
БЕЗПЕКИ
УКРАЇНИ


СЛУЖБА
БЕЗПЕКИ
УКРАЇНИ


СЛУЖБА
БЕЗПЕКИ
УКРАЇНИ
СЛУЖБА
БЕЗПЕКИ
УКРАЇНИ
СБУ

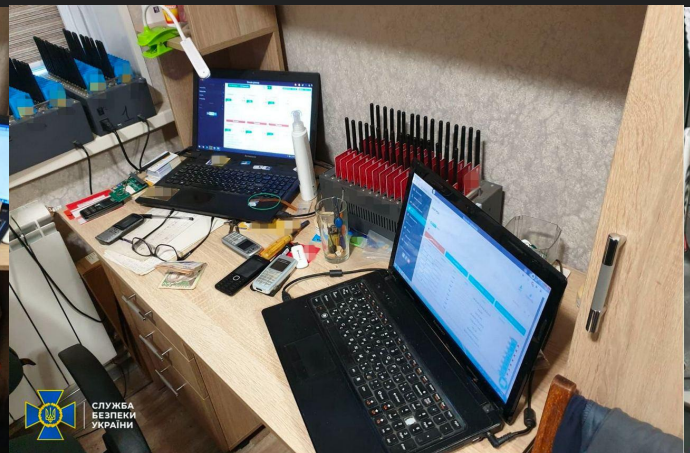
Operational use cases

- Social media accounts (Telegram, vKontakte, Instagram, etc.) to propagate stories produced by the GRU, FSB or pro-Russia media outlets, like, sharing, make large groups, etc.
- PSYOP/IOs (sending mass SMS to entire cities spreading disinformation, asking for surrender, providing details on how to support Russia, donations, etc.)
- COVCOM channel to stay in touch with agents or paramilitaries through anonymous Telegram channels and other E2E encrypted mobile apps
- DoS/flooding attacks on government/military
- Targeting high-value targets with IOs and/or CNE
- Proxies for bypassing content filtering of Ukraine



Limitations

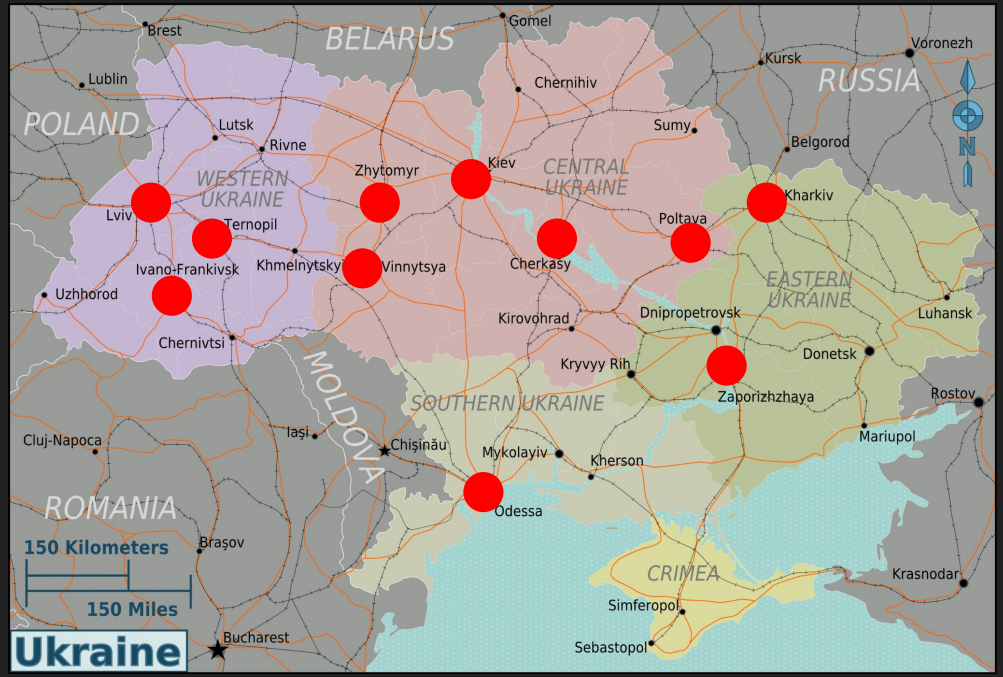
- Needs thousands of SIM cards, and lists of targets' numbers
- Relatively easy to discover them (transmitted signals, power consumption, triangulation of cellular comms, etc.)
- Very hard to measure the success of the IOs
- Requires operators with technical knowledge



Disrupted rogue cellular networks in Ukraine

since February 2022

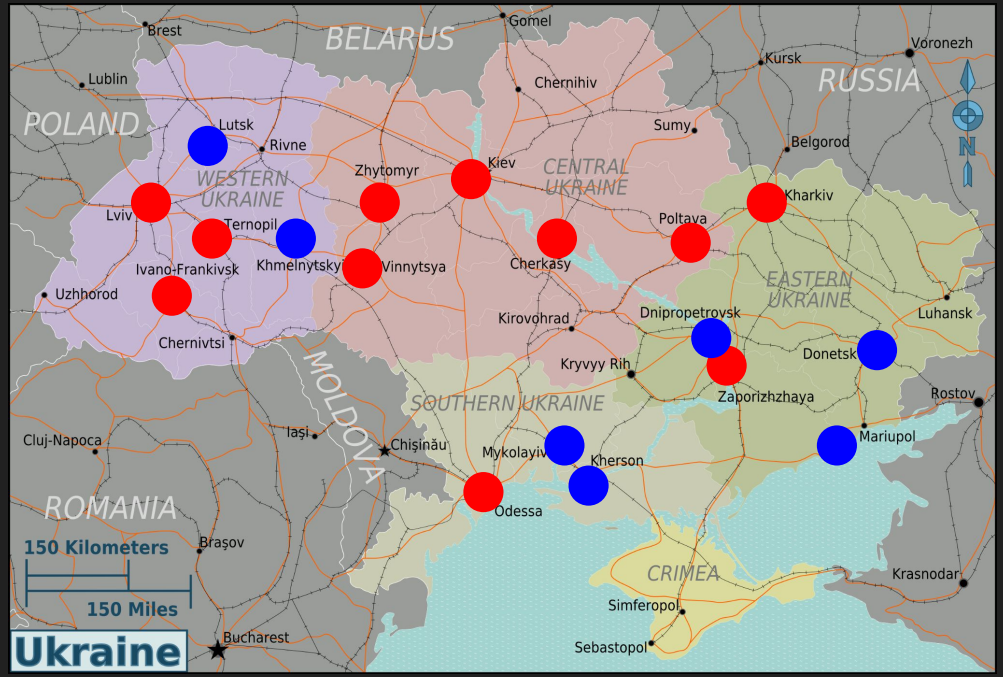
- 47 rogue cellular networks
  (SBU calls them “bot farms” (ботоферму)
  - 2+ million online accounts
  - Over 65,000 SIM cards

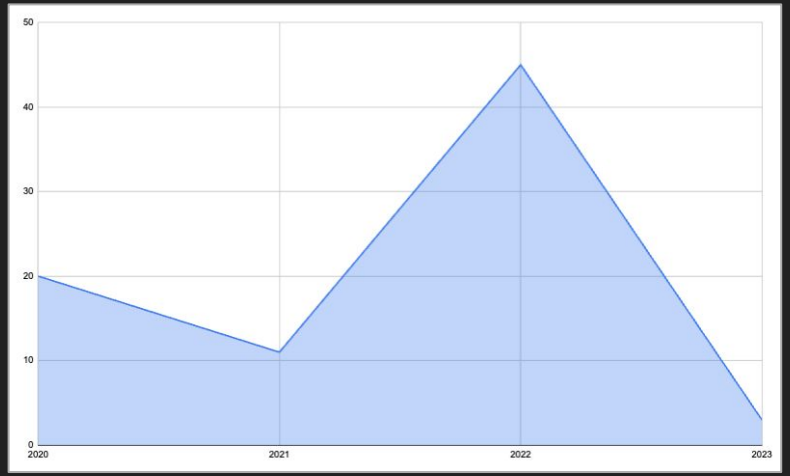


Disrupted rogue cellular networks in Ukraine

~~since February 2022~~

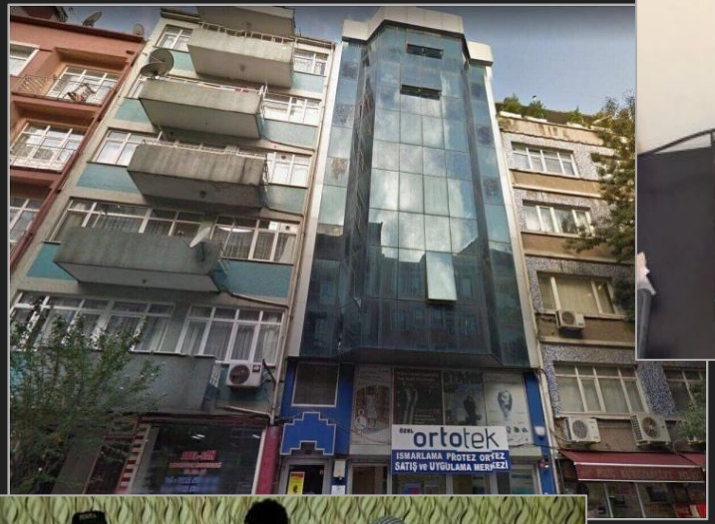
- Most disruptions were in Kyiv/Kiev (37.5%)
- On average each “farm” has 9300 SIM cards
- Most were part of PSYOP/IOs





- Anti-vaccine/COVID IOs
- Supporting LNR/DNR
- Anti-government messages
- Divisive subjects
- Support for Russian invasion

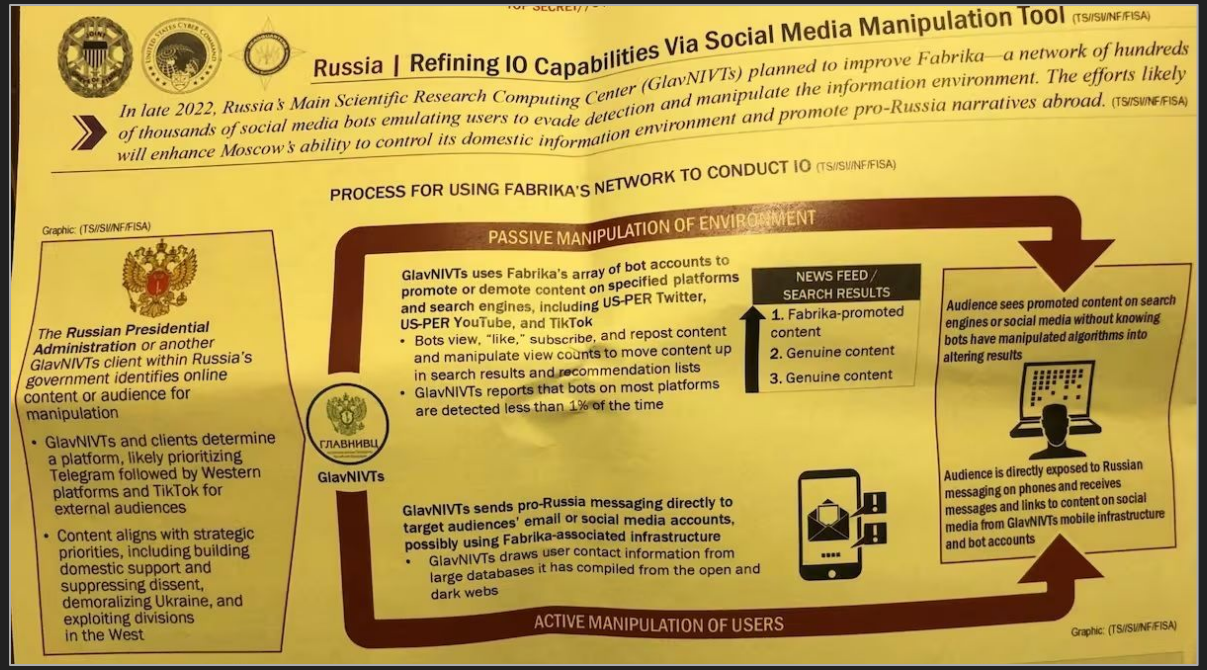
Is this known tradecraft?



Nov. 2017: Egyptian GIS disrupted a Turkish MIT spy ring of 29 people in Cairo

2016 and 2020:
Pakistani FIA disrupted illegal GSM gateways in Karachi used to set up covert communication channels

Is this known tradecraft?



Open consultation

Preventing the use of SIM farms for fraud

From: Home Office
Published 3 May 2023
Last updated 3 May 2023 — See all updates

Get emails about this page

Summary

This consultation sets out proposals to ban the manufacture, import, sale, hire and possession of SIM farms (devices for more than 4 SIM cards) in the UK.

This consultation closes at
5pm on 14 June 2023

Consultation description

SIM farms are devices that can hold multiple SIM cards, which are used to:

- send scam texts
- run scam call campaigns
- post misleading, false or phishing messages on social media in bulk

We're seeking views on:

- our definition of SIM farms, to ensure it accurately captures the devices currently in use
- our plan to apply the measure only to devices with more than 4 slots
- whether other technologies used almost exclusively to commit fraud should be included

Thank you!

@xorlgr
Anastasios Pingios
Spy News
Spy Collection