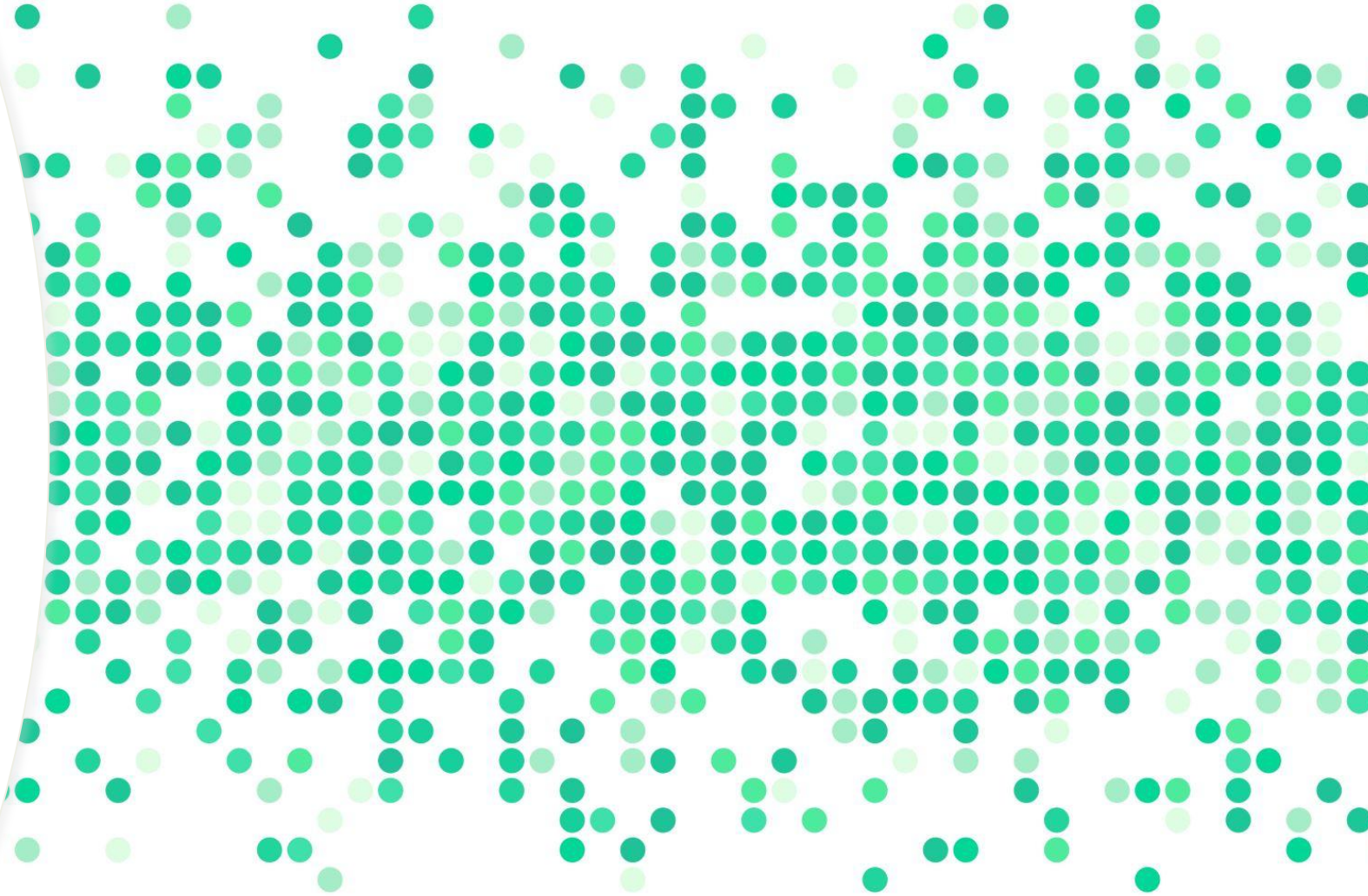
# Russia's Open-Source Code and Private-Sector Cybersecurity Ecosystem

Justin Sherman

for Margin Research

October 28, 2022



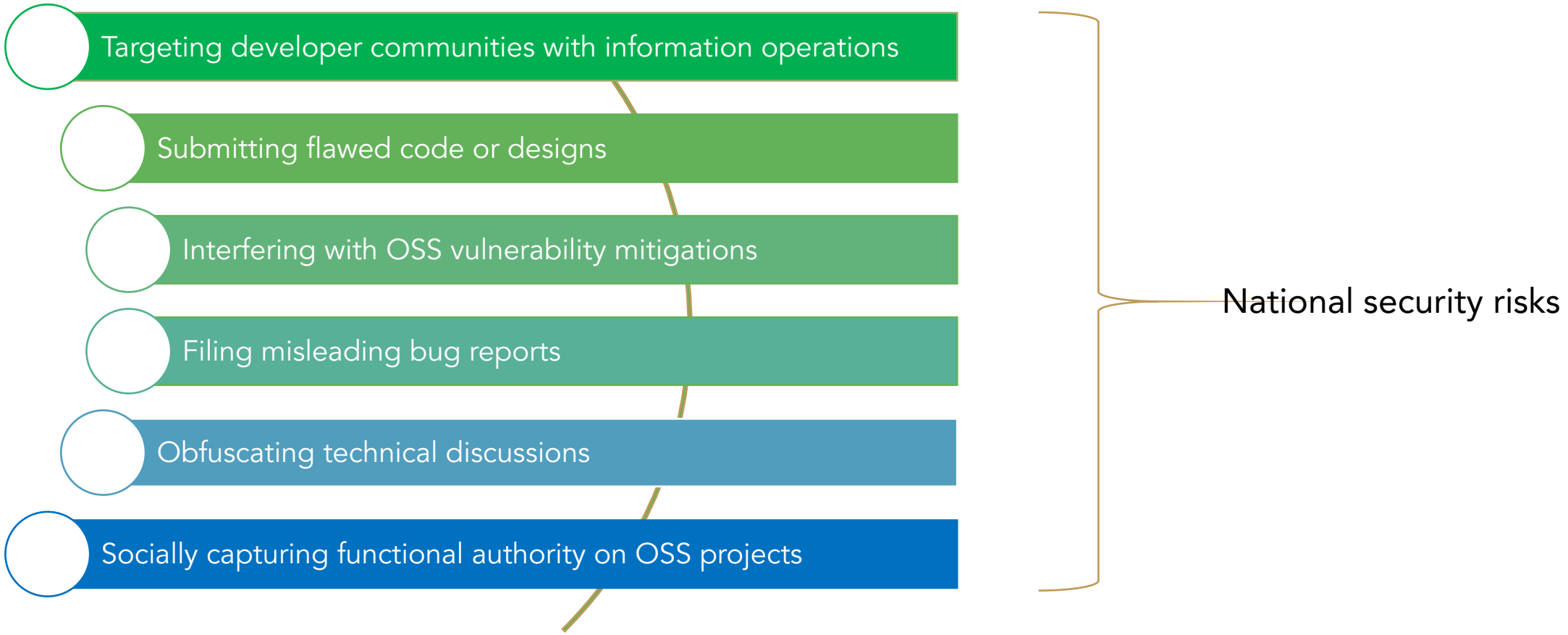
# This Talk

- Margin Research's SocialCyber Project
- Russian Open-Source Code
- Russian Private-Sector Cybersecurity Actors
- What Now?

# Margin Research and SocialCyber

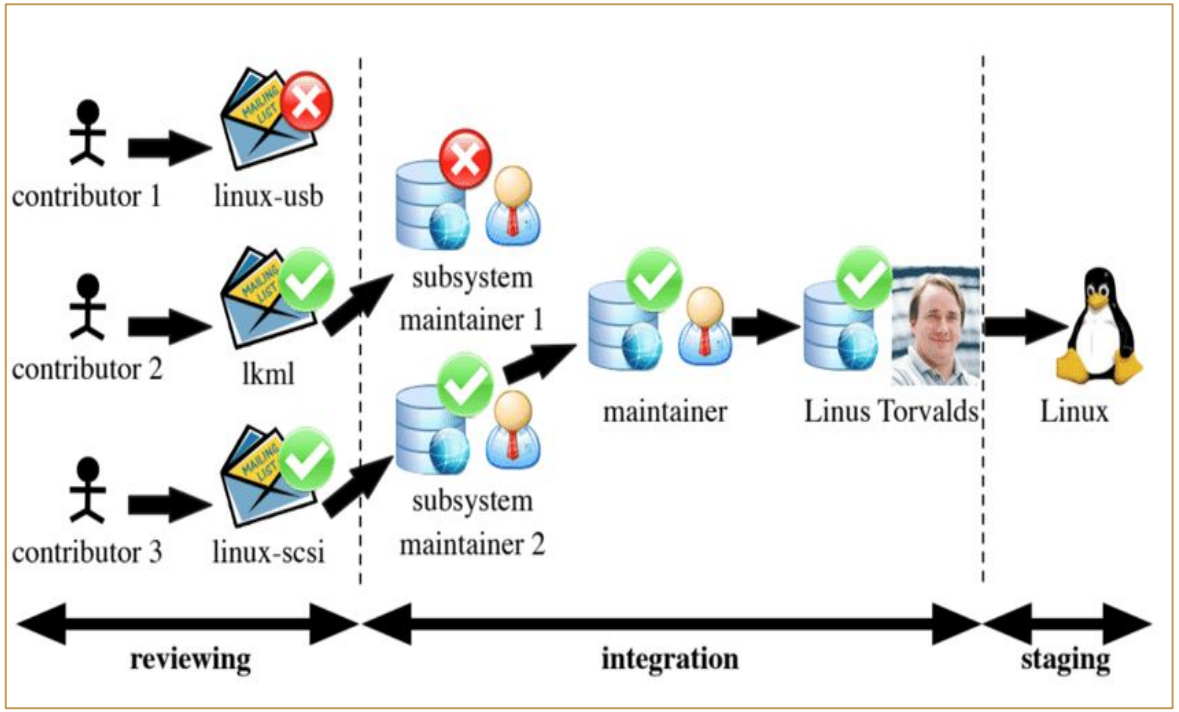
- Margin Research: boutique NYC-based security firm
- SocialCyber — DARPA's Hybrid AI to Protect Integrity of Open Source Code project
  - DOD relies heavily on open-source software (OSS)
  - How should we think about protecting that ecosystem and understanding threats posed to it?

# How might malicious actors interfere with OSS?

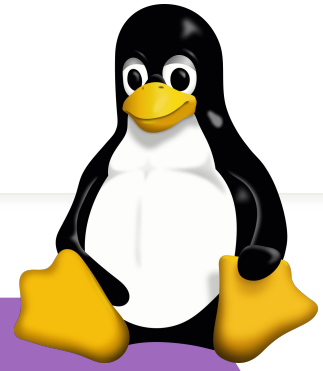


# Margin's Approach: Analyze the Linux Kernel

- Linux is composed of subsystems run by maintainers ("a lieutenant system built around a chain of trust")
- Explicitly defined maintainers list with contact information



# Analyze the Linux Kernel (cont.)



## Phase 1

### Ingestion

- Ingest data into Dgraph
- Create appropriate schema to represent Git code in graph

## Phase 2

### Correlation

- Connect otherwise disparate pieces of data to inform the dataset
- *Ex.* Twitter information
- *Ex.* Linux Kernel mailing list data
- Build capability to search for names

## Phase 3

### Comprehension and Annotation

- Characterize threat
- Use regional / subject matter experts to identify specific individuals and organizations of particular interest
- Manual analysis with build towards possibility of more automation

# Initial Findings


- Chinese telecom
- US-designated national security threat
- 2021: top contributor to Linux Kernel (beat Intel)

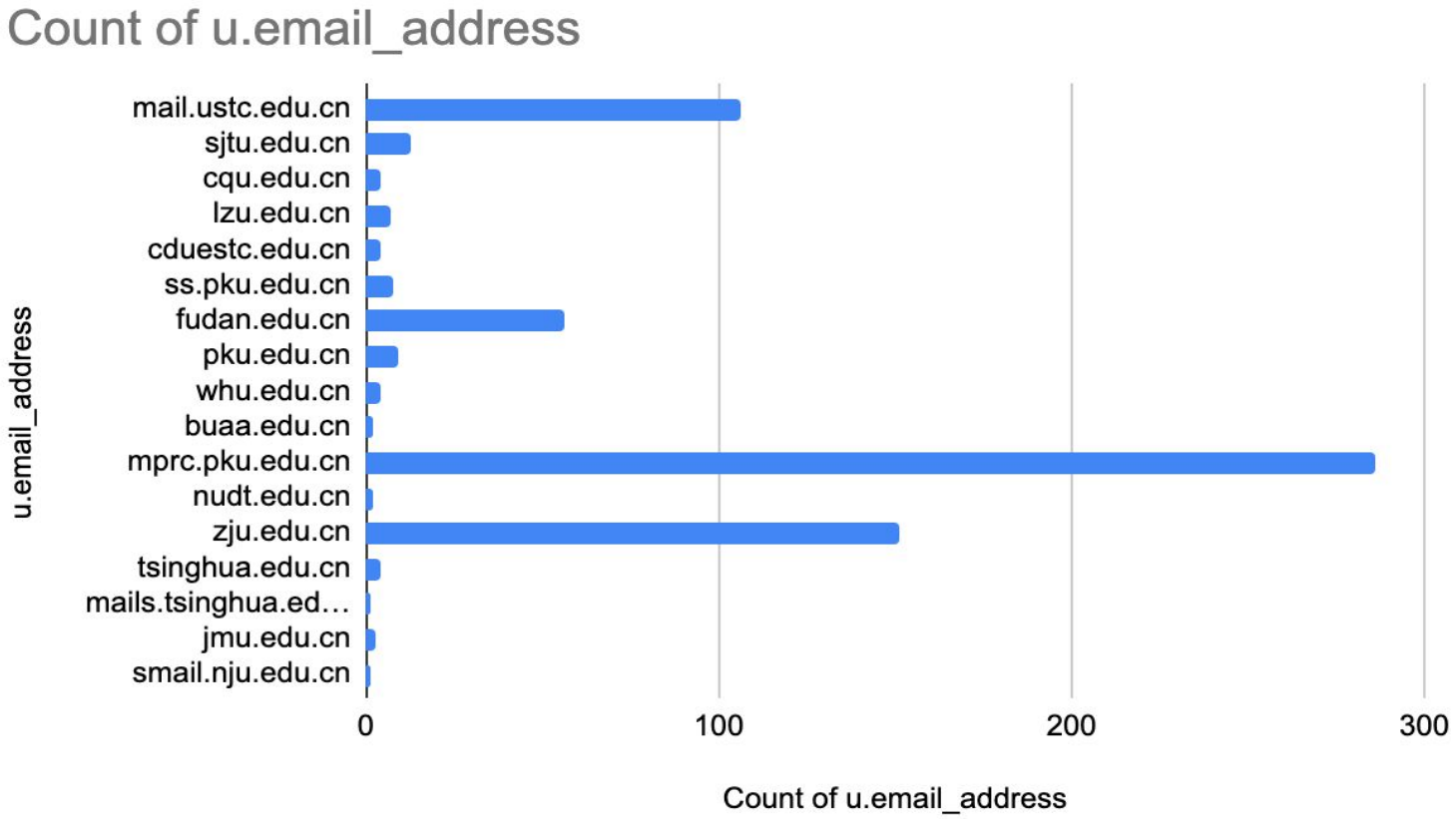

- US-sanctioned Russian cybersecurity firm (more later)
- Key Linux Kernel contributor

- Also: of 36,000 contributors to Linux kernel, identified 30 exhibiting suspicious behaviors
- Several are known to submit code with exploitable vulnerabilities into the kernel

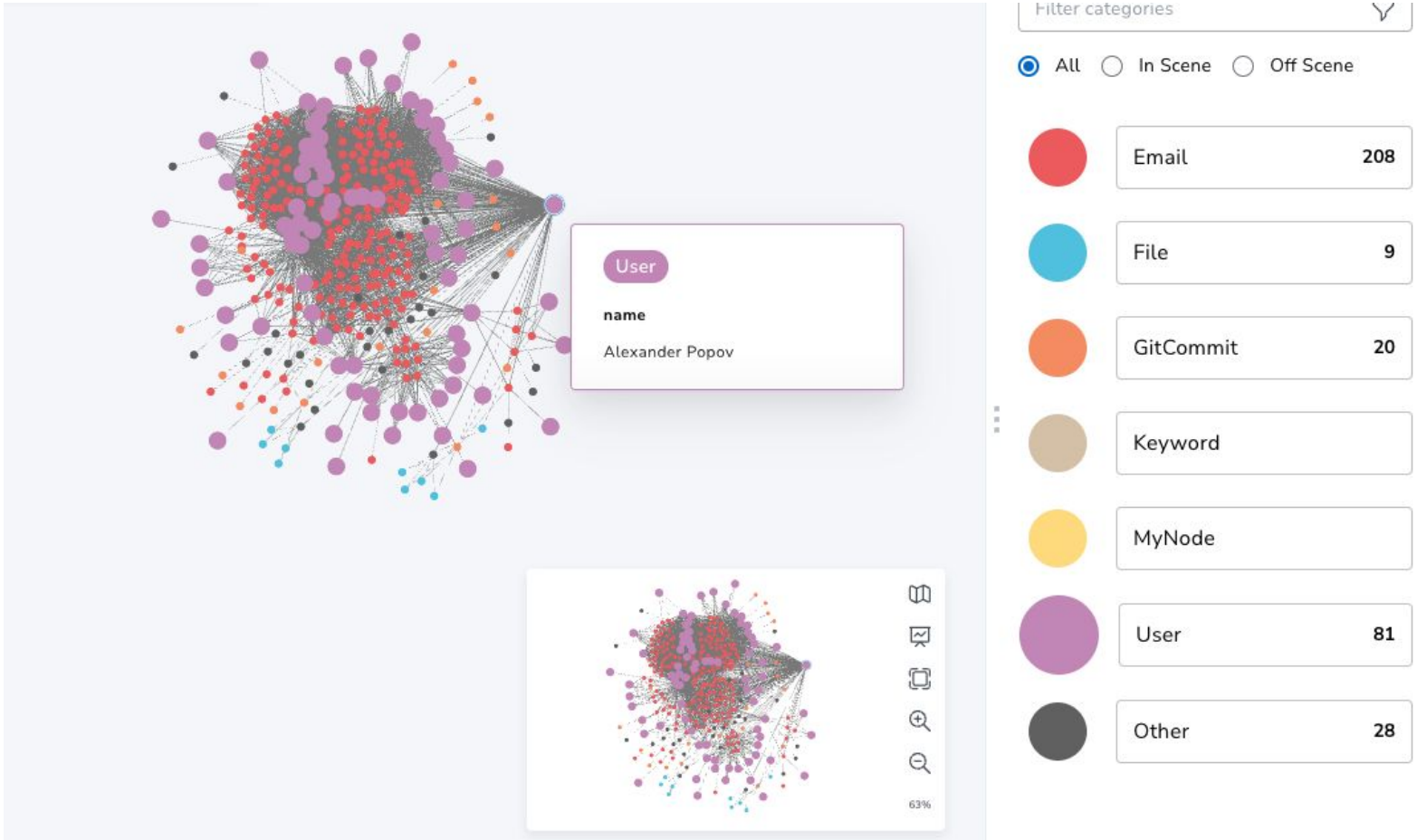
- *Ex.* 2020: Huawei senior security engineer publishes a commit to the Linux Kernel Self-Protection Project
- Claimed it was a security patch
- "Patch" was filled with introduced vulns
- Huawei denied responsibility for the commit

# Initial Findings (cont.)

Total volume of contributions to the Linux Kernel from Chinese educational institutions



# Initial Findings (cont.)

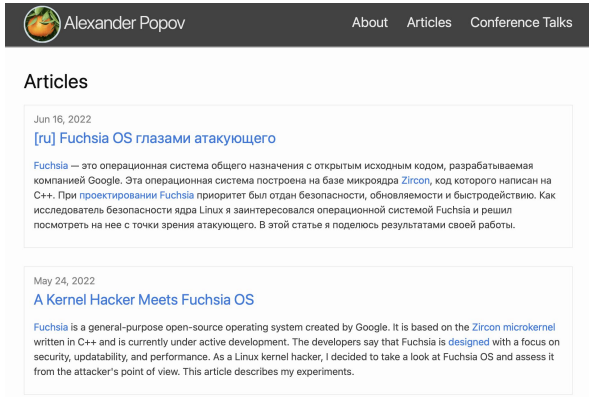


# Initial Findings (cont.)

Alexander Popov

- Now: Principal Security Researcher, Positive Technologies
- Past: Linux Kernel Developer and Security Researcher, Positive Technologies
- Education: Information Security, Moscow State University of Railway Engineering

Blog, largely on Linux security:




40+ patches accepted into mainline Linux Kernel

Found and fixed local privilege escalation flaws in Linux Kernel

- CVE-2021-26708
- CVE-2019-18683
- CVE-2017-2636

Speaker at OffensiveCon, Nullcon, Linux Security Summit, Zer0Con, Positive Hack Days, ZeroNights, Linux Plumbers, and others

Contributions are security-focused; work appears defensive

# Linux and Moscow's Domestic Tech Push

## 2010-2014

Growing Kremlin paranoia about the internet (Arab Spring, Snowden leaks, Euromaidan, …)

Domestic tech push grows

## 2015-2021

Laws, policies on domestic tech

Incentives for domestic IT firms

May 2015: Russia's Skolkovo plan faces budget cuts, deteriorates (started 2009)

Sep. 2017: Putin calls on Russian tech firms to watch their imports of foreign tech

May 2019: Russia grants highest security rating to Astra Linux, allowing MOD and IC to use the software

## 2022-Now

Russian government accelerates expulsion of Western technology, technology platforms

Kremlin exempts certain IT workers from military draft

July 2022: Astra Linux announces planned Moscow IPO

# Private-Sector Russian Actors

- Private-sector cybersecurity companies in Russia:
  - Front companies for security services
  - Building talent
  - Developing capabilities
  - Supporting state operations
- Russian cyber power draws on the vast, tangled web of Russian cyber actors — including companies

# From Small Vendors to Large Suppliers

kaspersky

POSITIVE TECHNOLOGIES

NTECH LAB

SOVCOMBANK

BI.ZONE Cybersecurity

СБЕРБАНК ТЕХНОЛОГИИ

INFOWATCH®

ANGARA SECURITY

SWORDFISH SECURITY

SECURITY VISION

Ростелеком Солар

# Support May Be Defensive

SECURITY code

FSS of Russia

The Ministry of Defence of the Russian Federation

The Ministry of Internal Affairs of Russia

EMERCOM (Federal Rescue Service) of Russia

The Ministry of Justice

The Russian Prosecutor General

The Federal Security Guard Service of the Russian Federation

Rosgvardia

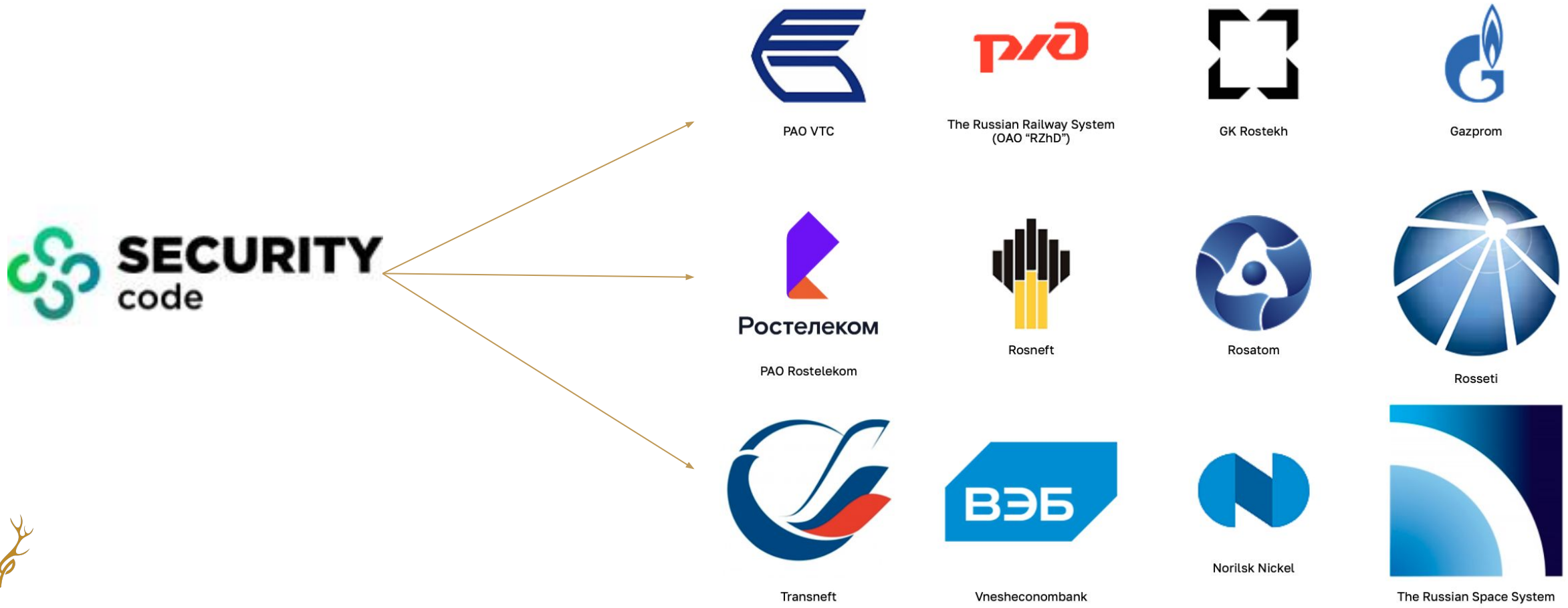
The Federal Penitentiary Service of Russia

The Investigative Committee of the Russian Federation

The Russian Constitutional Court

The Supreme Court of the Russian Federation

# Support May Be Defensive (cont.)



# Support May Be Offensive

- Neobit, AST — covert capability support (US Treasury)
  - June 2010 — US expels Russian spy working at Microsoft
  - Individual previously worked at Neobit

- Positive Technologies — capability development (Treasury)

# Case Study: Positive Technologies

CEO: Denis Baranov
(Денис Баранов)

CTO: Dmitry Kurbatov
(Дмитрий Курбатов)

Director of Engineering: Alexey Andreev
(Алексей Андреев)

POSITIVE TECHNOLOGIES

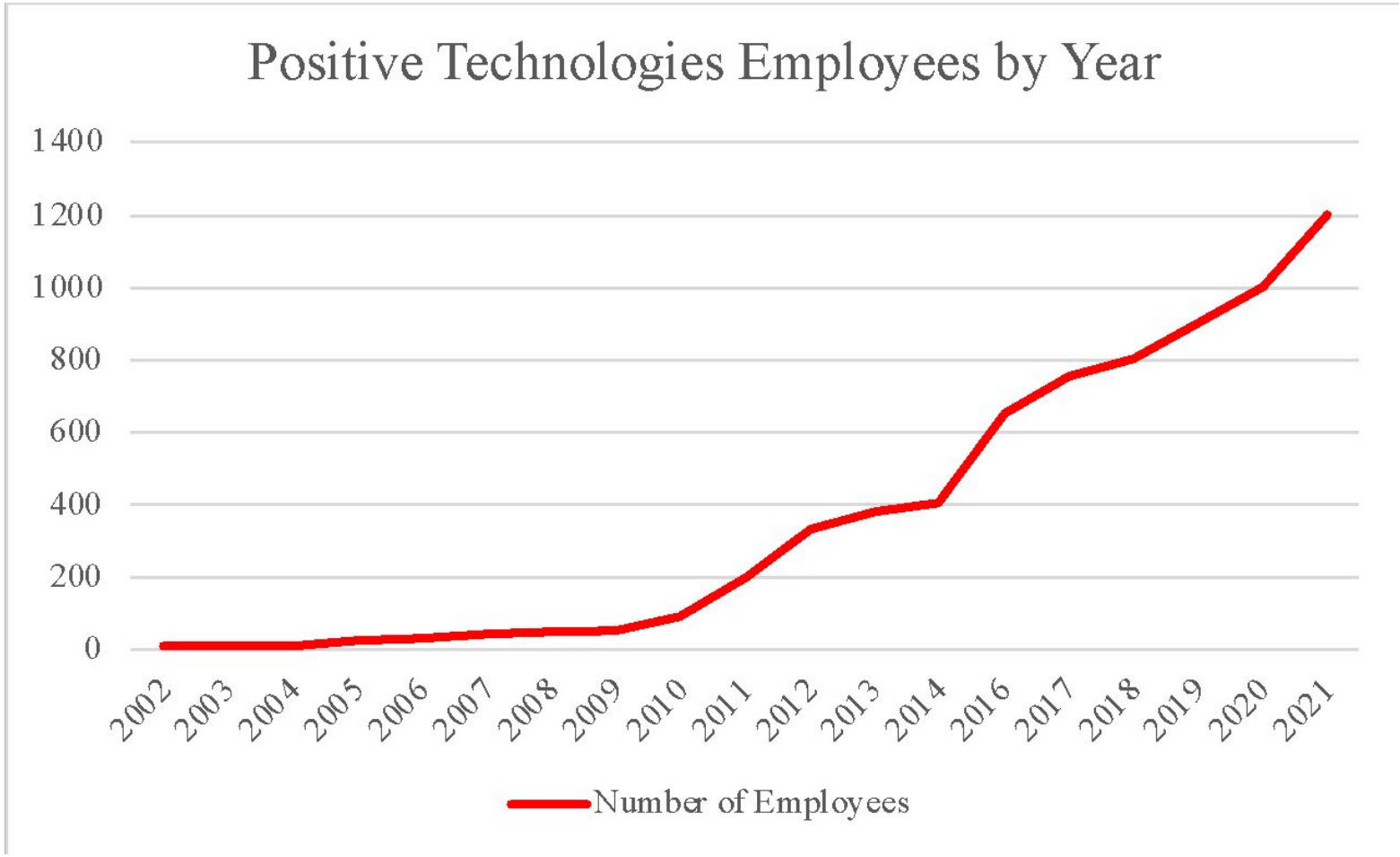
- Founded in 2002
- Positive: PT supports MOD
- USG (publicly): PT supports FSB cyber operations
- USG (privately): PT works with FSB on exploit discovery, malware development, and reverse engineering of Western (incl. US) capabilities
- Helps FSB, GRU recruit hackers
- Content used in 65+ universities
- Largest Russian annual CTF

Head of Board of Directors, former CEO: Yury Maksimov
(Юрий Максимов)

Head of Reverse Engineering: Dmitry Sklyarov
(Дмитрий Скляров)

Head of Vulnerability Management: Ilya Egorkin
(Илья Егоркин)

# Positive Technologies (cont.)



# Positive Technologies (cont.)

Denis Baranov (Денис Баранов)
- CEO (as of July 2021)
- Before that, R&D Director for Application Security @ Positive
- Joined Positive in 2010
- Driving force between Positive's "The Standoff," a cyber competition for Russian hackers

Three CEO priorities:
- Increase innovation around automated attack defense
- Launch IPO
- Scale up international presence (est. 40-50% int'l growth from 2020-2021)

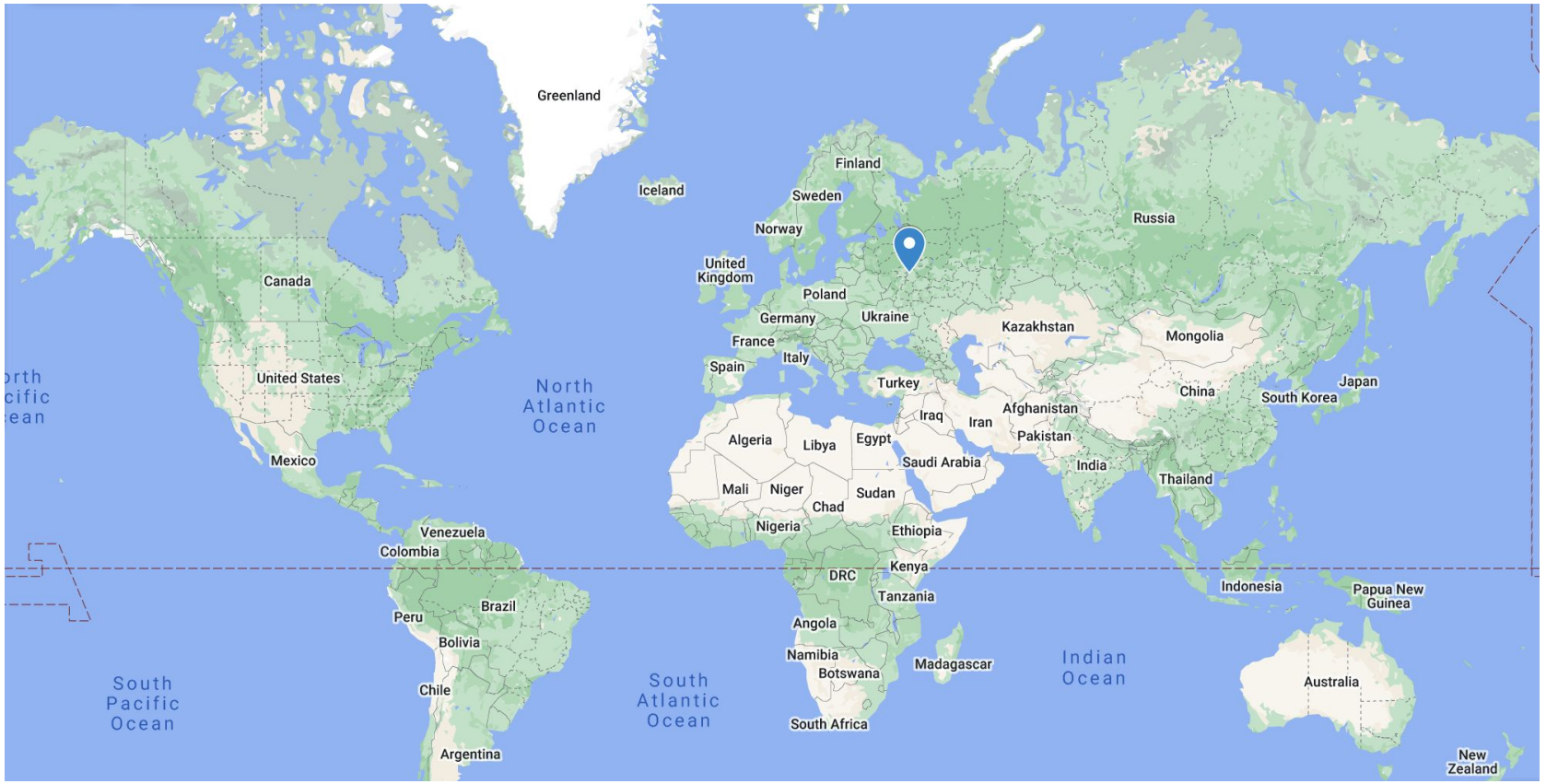
Positive Technologies: Вероятна международная экспансия

Рынок Акций

- Positive wants to expand into Southeast Asia, South America, Arab countries
- Russia, US, Israel, China are four countries with substantial cybersecurity products/services
- E.g., Latin American vendor might want to diversify risk to US + Russian cybersecurity products

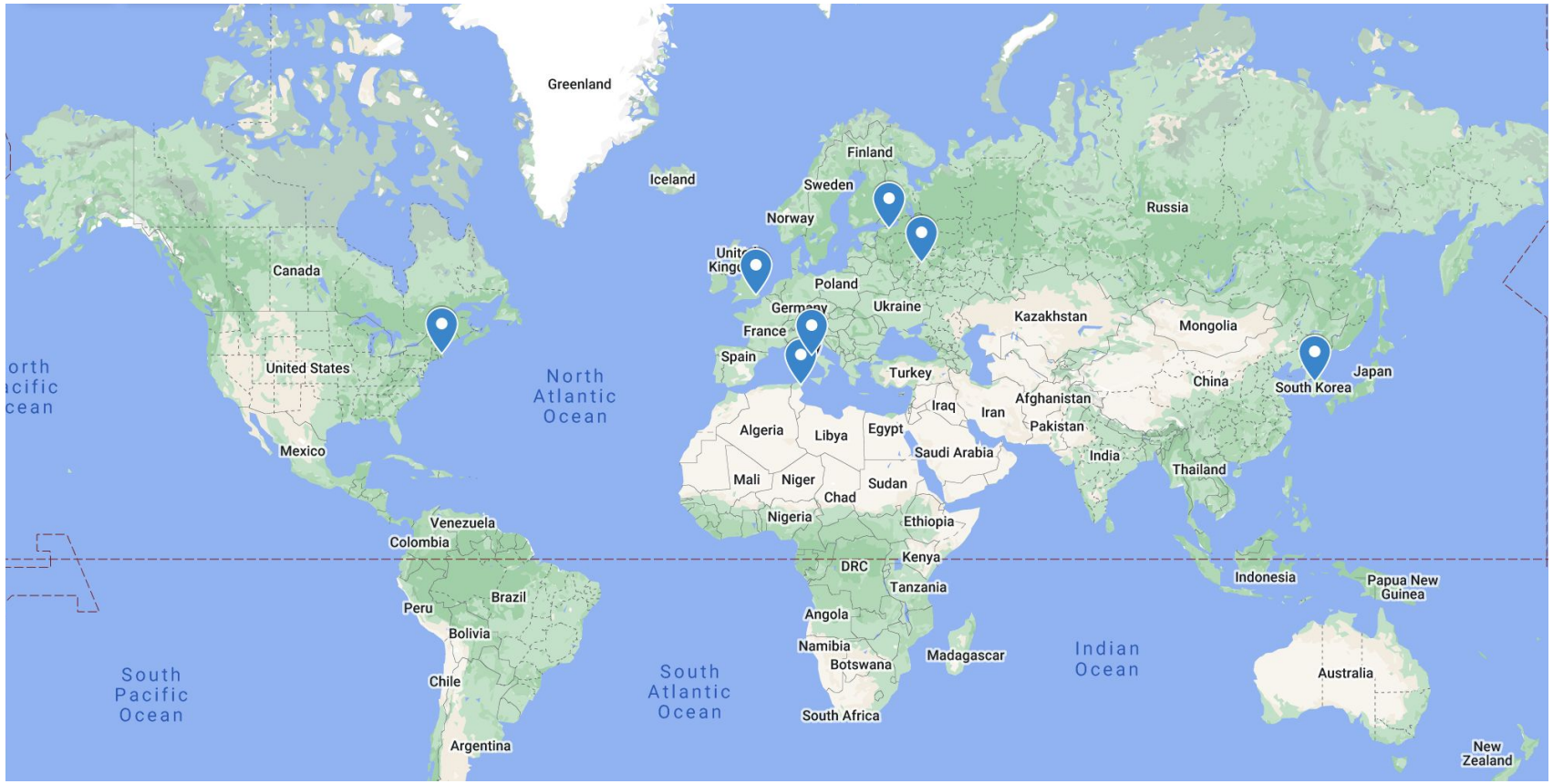
# Positive Technologies (cont.)

2002: Moscow office



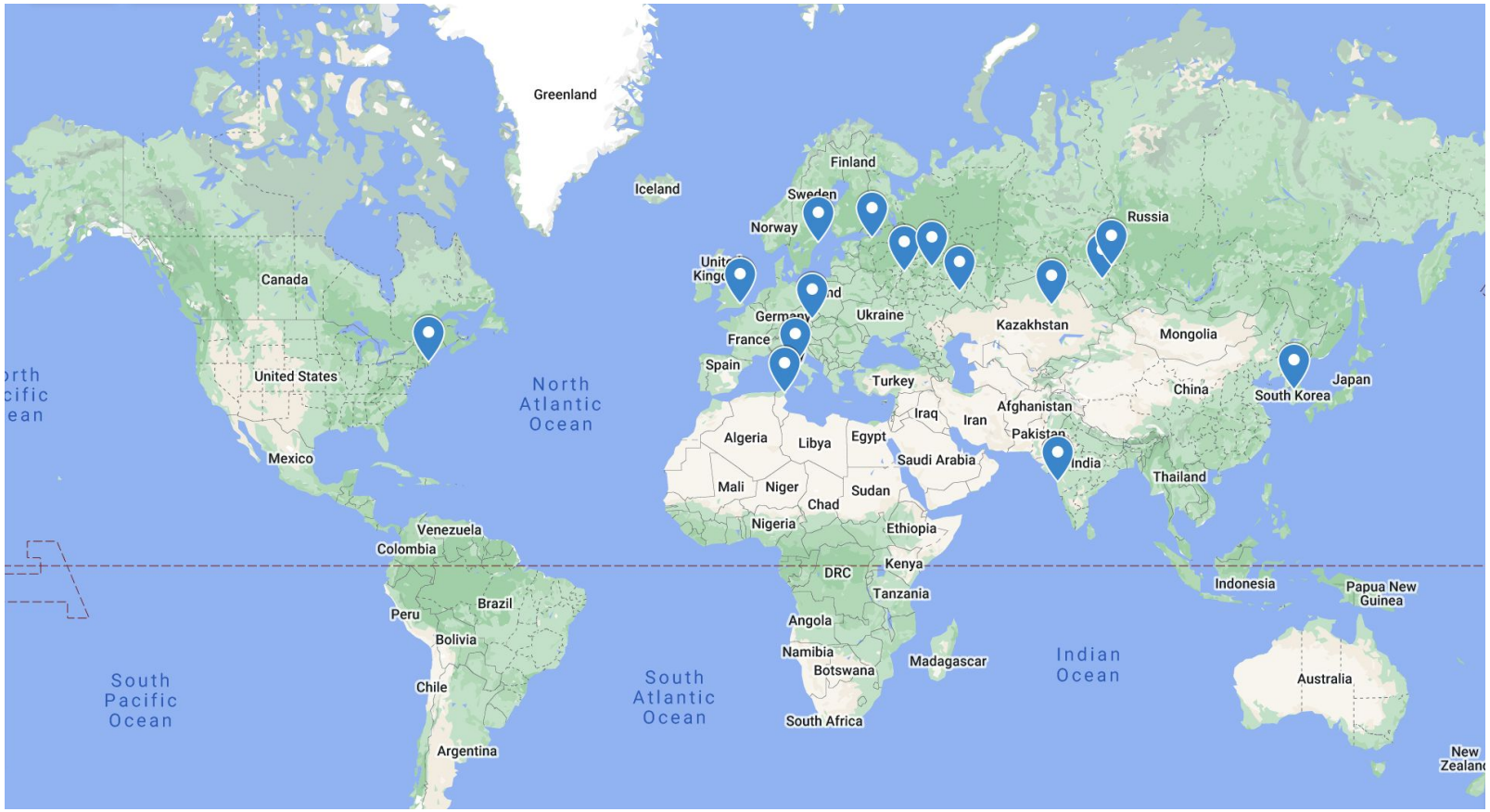
# Positive Technologies (cont.)

2012: St. Petersburg office + Boston, Tunis, Rome, Seoul, London offices



# Positive Technologies (cont.)

2021: new offices in Mumbai, Czech Republic, and more



# Positive Technologies (cont.)

Dmitry Sklyarov (Дмитрий Скляров)

- Positive Technologies — Head of Reverse Engineering
- 47 years old (born 12/18/1974)
- Widely spoken at Russian security conferences
- Been with Positive since ~2008

July 16, 2001— Arrested by FBI at DEFCON for violating the DMCA

→ Agreed to testify against his employer ElcomSoft distributing the circumvention software

→ December 13, 2001— US let Sklyarov return to Russia

→ Joined Positive Technologies at least in 2008

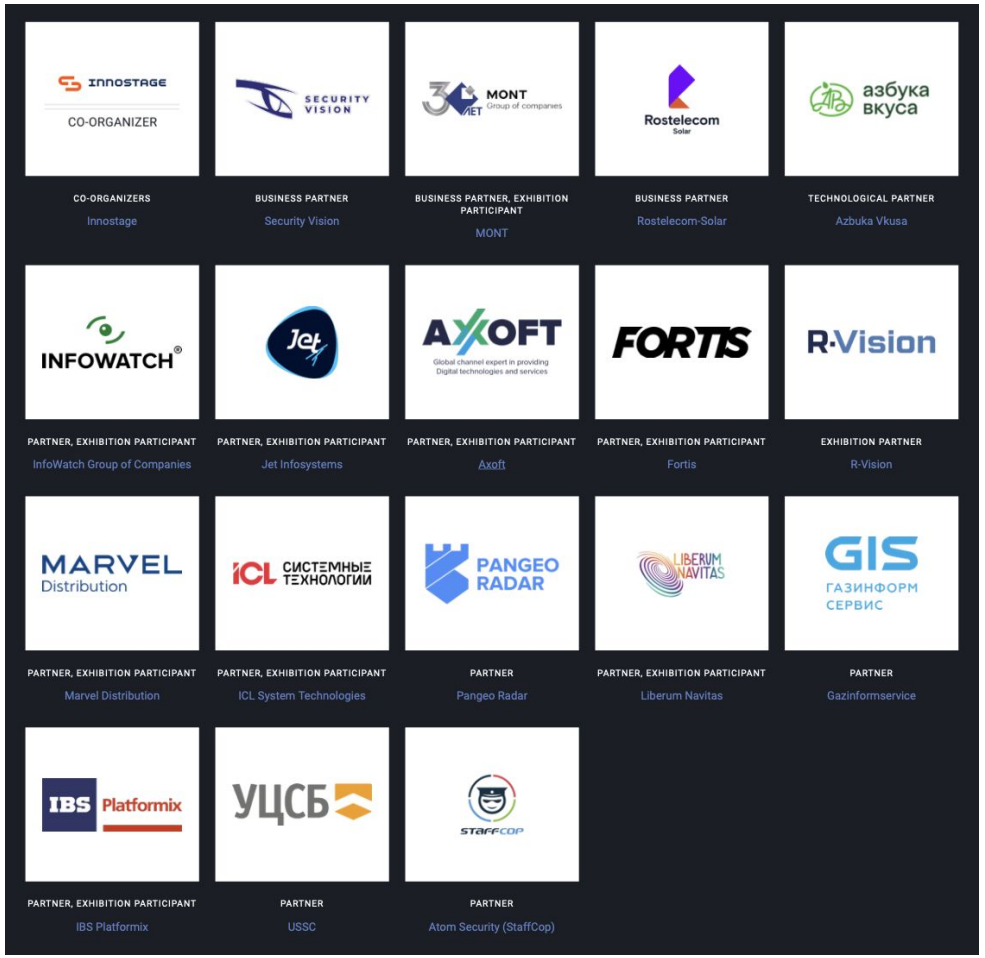
→ Running major Positive Technologies research efforts

→ Identifying and disclosing vulnerabilities in Intel chips, Mitsubishi controllers, US industrial energy systems, more

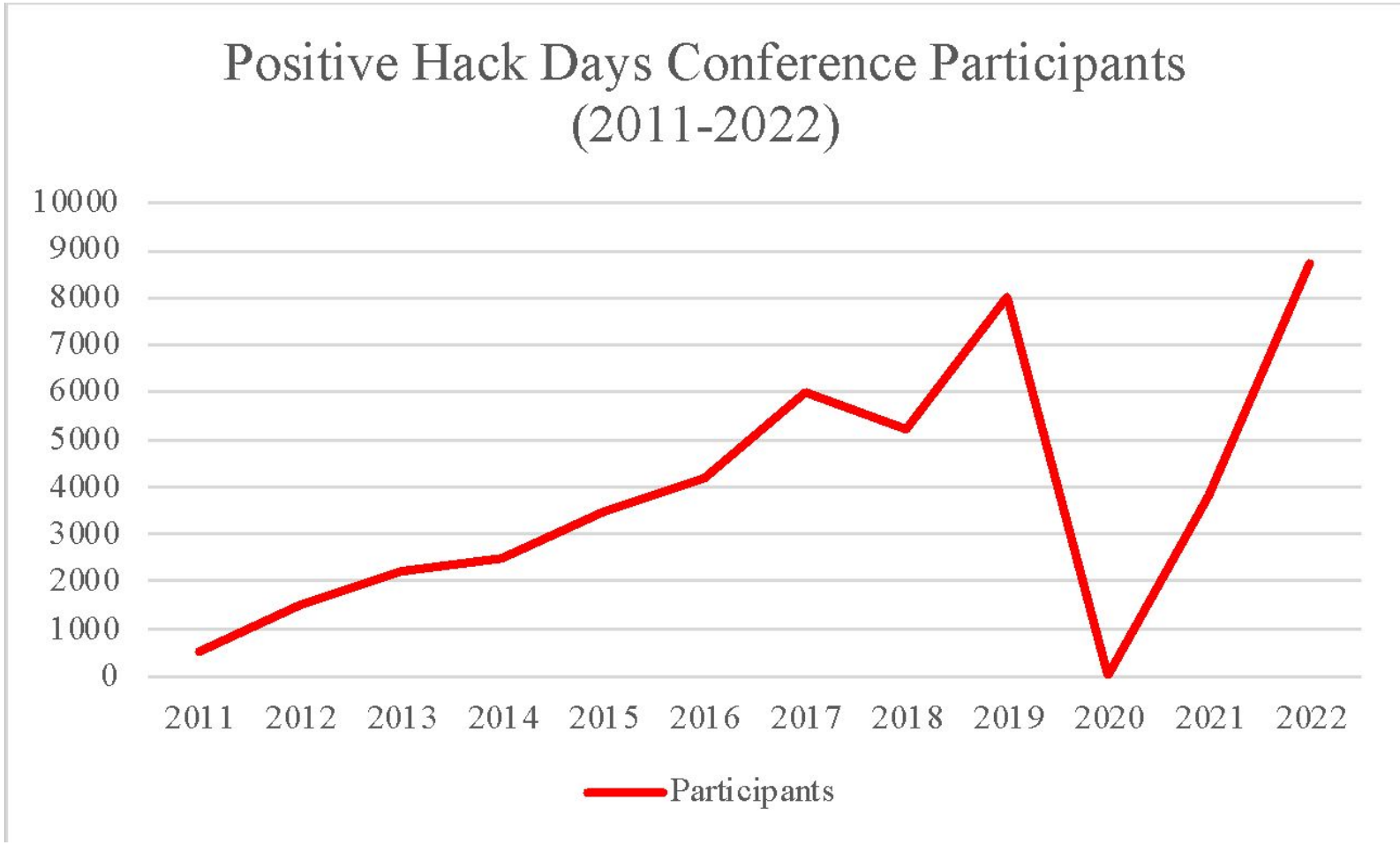
→ Supporting conference (e.g., Russian IC recruiting) events

# Recruitment: Positive Hack Days

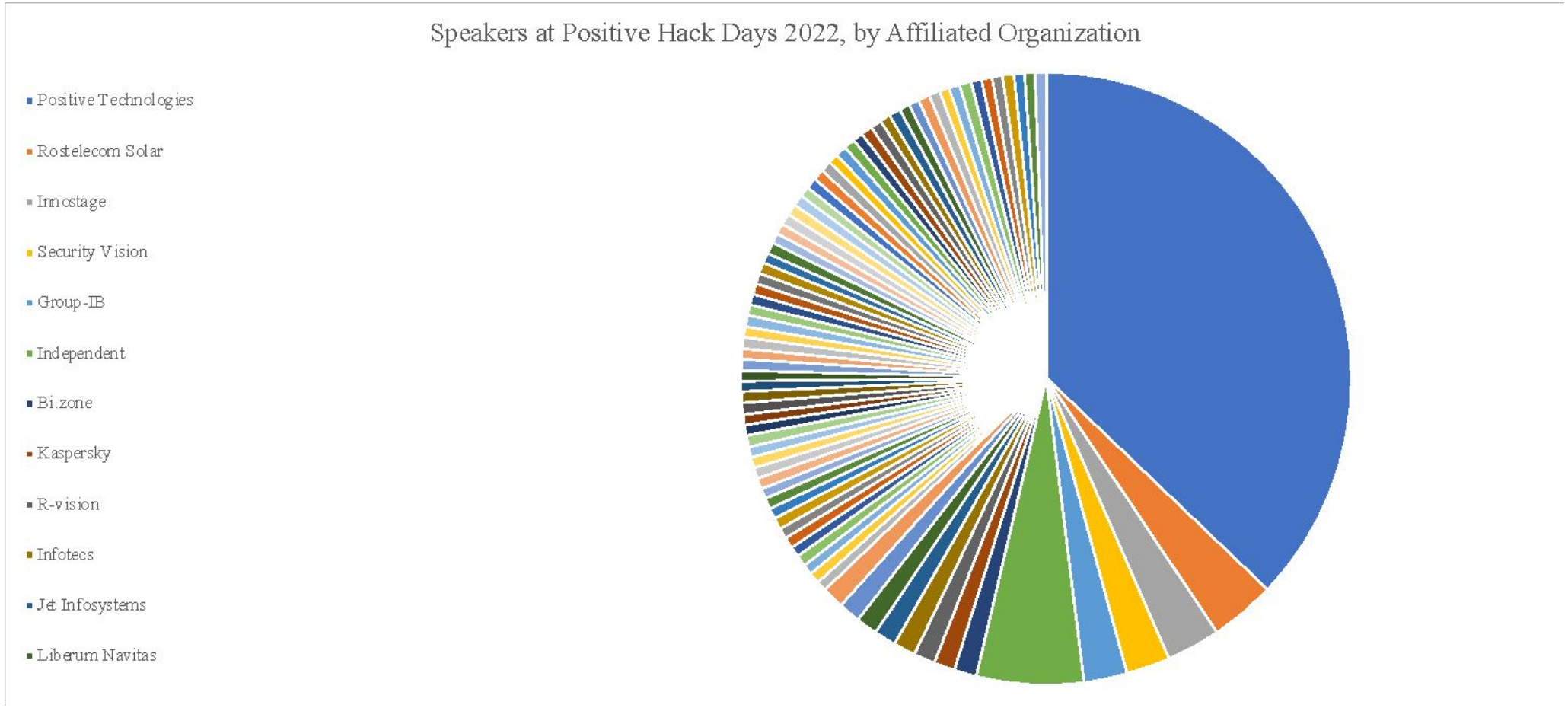
- Conference and CTF started by Positive Technologies in 2011
- FSB, GRU use to recruit
- Numerous sponsors and partners from the Russian cyber community (see: right)



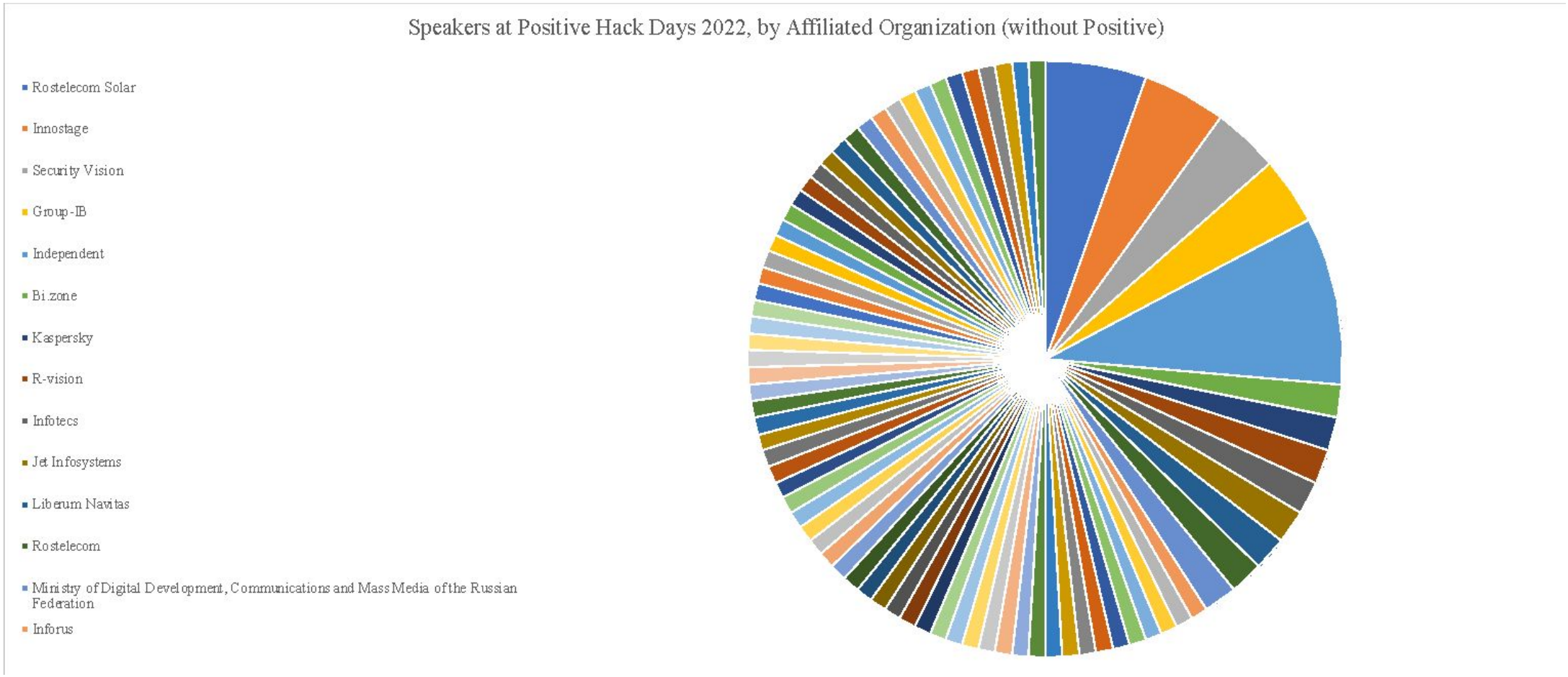
# Positive Hack Days (cont.)



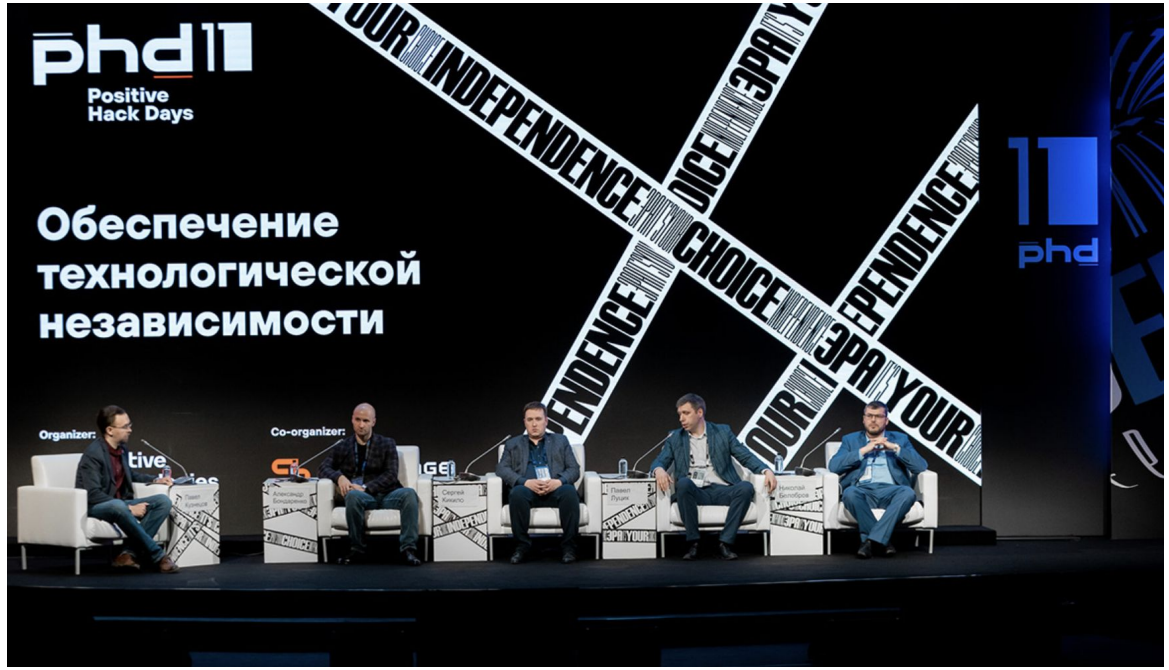
# Positive Hack Days (cont.)



# Positive Hack Days (cont.)



# Positive Hack Days (cont.)




- 2022 event — 8,700 attendees; 100 talks; cyber simulation
- Speakers included Maria Zakharova (Russian MFA); Minister of Digital Development, Communications, and Mass Media; 2 from Rostelecom; 1 from Mozhaisky Military Space Academy
- Oleg Skulkin @ Group-IB (Singapore-based w/ local RU entity) — the world hacking company sees Russia as fair game
- Cybersecurity director @ Russian Min. of Digital Development — need to expand RU bug bounty platforms, like Standoff 365

# Recruitment: Moscow CTF


- 2010 — Russia's Association of Chief Information Security Officers launches competition
- 2010 — FSB begins using event to recruit hackers
- 2015 — MOD begins sponsoring event (and recruiting)
- 2021 — sponsors range from Voentelekom (telecom equipment supplier) to Infotecs (on US Entity List for enabling malicious Russian cyber activity; also works with FSB; has links to Russian businessperson allegedly supporting influence operations)

# Entanglement: Skolkovo CTF Russian Cup

- Started by Skolkovo Innovation Center, set up in 2010 by Dmitry Medvedev as a Russian Silicon Valley
- Semi-imploded due to corruption, Putin budget cuts
- Runs 46 hacker competitions across Russia in 20 different cities, with over 3,500 hackers in most recent cup round
- Judges come from US-sanctioned cybersecurity companies, weapons developers (e.g., Kronstadt Group), others

# What Now?

- SocialCyber project continues to evolve
- Other, future workstreams could include:
  - Increased automation of capabilities
  - Expanded analysis to focus on other open-source software
  - Expanded analysis beyond China, Russia, Iran
  - Deep-dives into specific companies and other actors
  - Deep-dives into specific foreign bug bounty programs

# Questions?

@Margin_Research

@jshermcyber