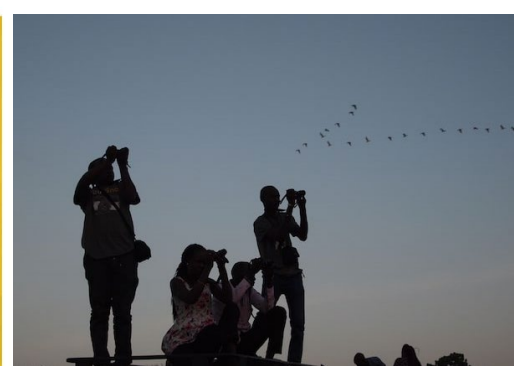
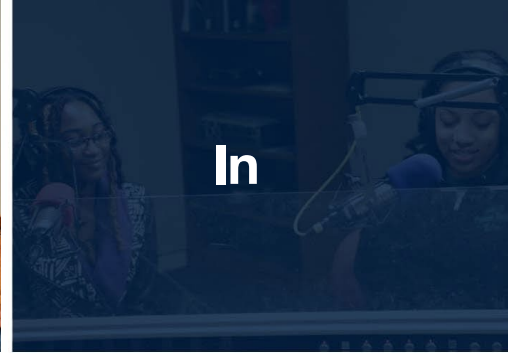
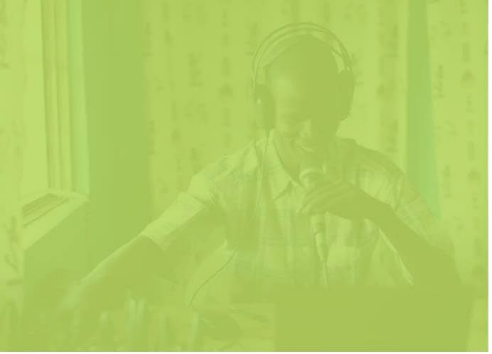




Digital threats against civil society in the rest of the world

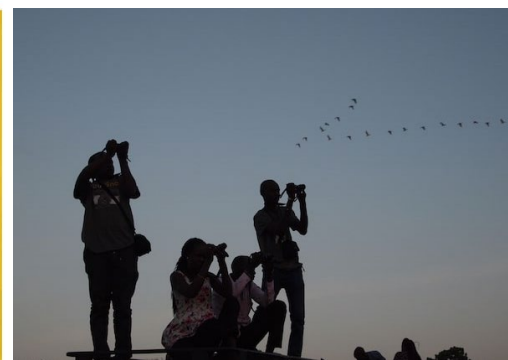
Martijn Grooten, Internews
Botconf 2023, Strasbourg, France





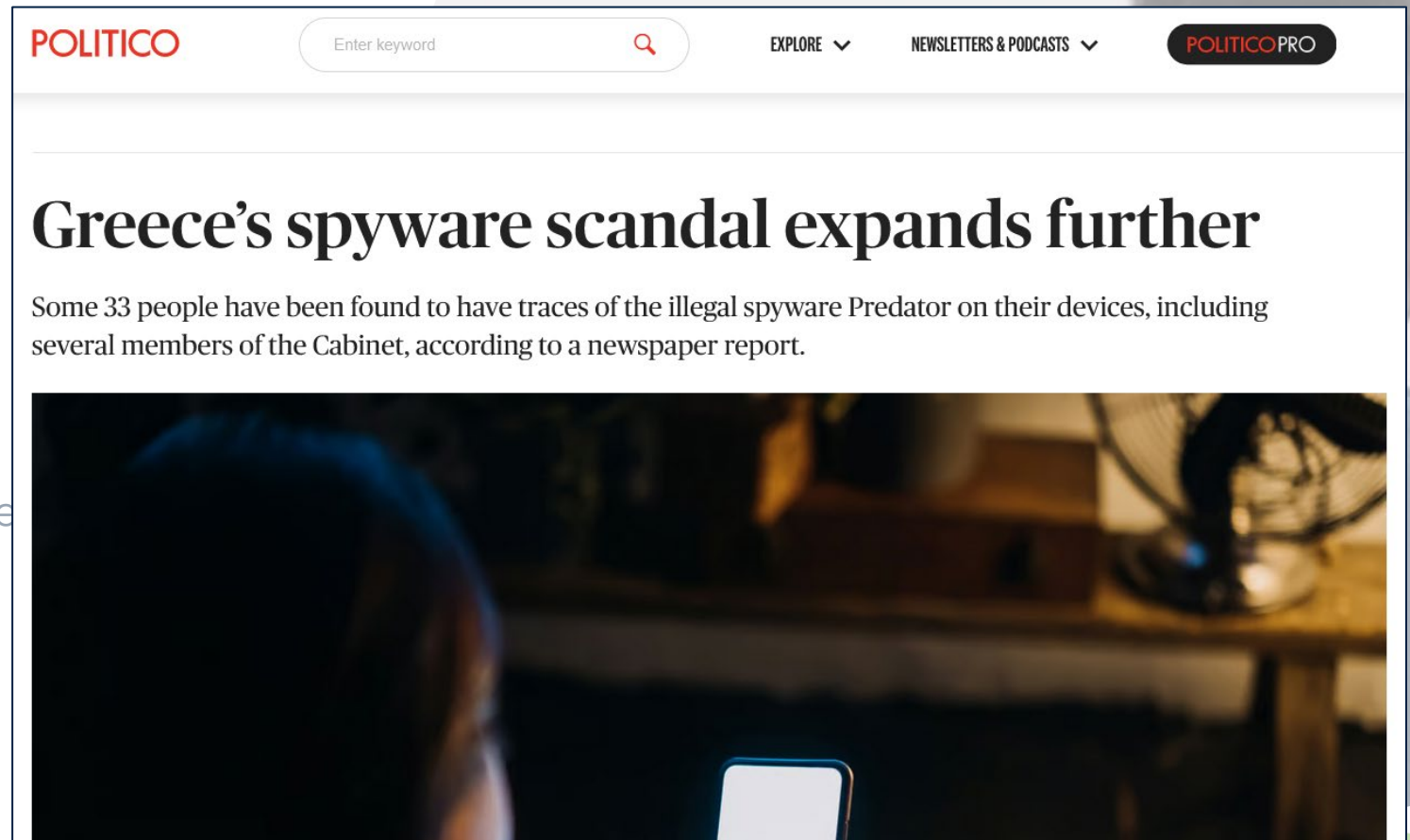
Digital threats against civil society in the rest of the world

Martijn Grooten Interviews
Botconf 2023, Strasbourg, France



About me

- Mathematician
- Netherlands -> UK -> Greece
- Virus Bulletin (2007–2019)
- Botconf speaker (2014, 2019)
- Coalition Against Stalkerware, other projects
- Internews (2022–)



We support independent media in **100 countries**



Photo by Kim Nguyen van Zoen

- 1** Tools journalists need to survive and thrive
- 2** Deep and authentic local partnerships
- 3** Global reach, especially where information is most needed

Internet Freedom & Resilience team

- Journalist security
- Organizational security ('orgsec')
- Anti-censorship/-shutdowns
- Open-source tools
- Digital rights
- Digital threats

etc.



Civil Society

- Media organizations and journalists
 - Human rights organizations
 - Women's rights, LGBTQ+ rights, indigenous rights, religious rights etc.
 - Trade unions
 - Hobby and sports clubs
- etc.



The Rest of the World

“Non-Western countries”:

- Asia
- MENA (Middle East and North Africa)
- Africa
- LAC (Latin America and the Caribbean)
- Eastern Europe

Related term: “Global South”



Civil Society in the Rest of the World: the context

- Censorship and Internet shutdowns
- Surveillance
- Misinformation/disinformation
- Harassment
- Complex relationship with government
- Non-digital threats: arrests, violence, intimidation, murder

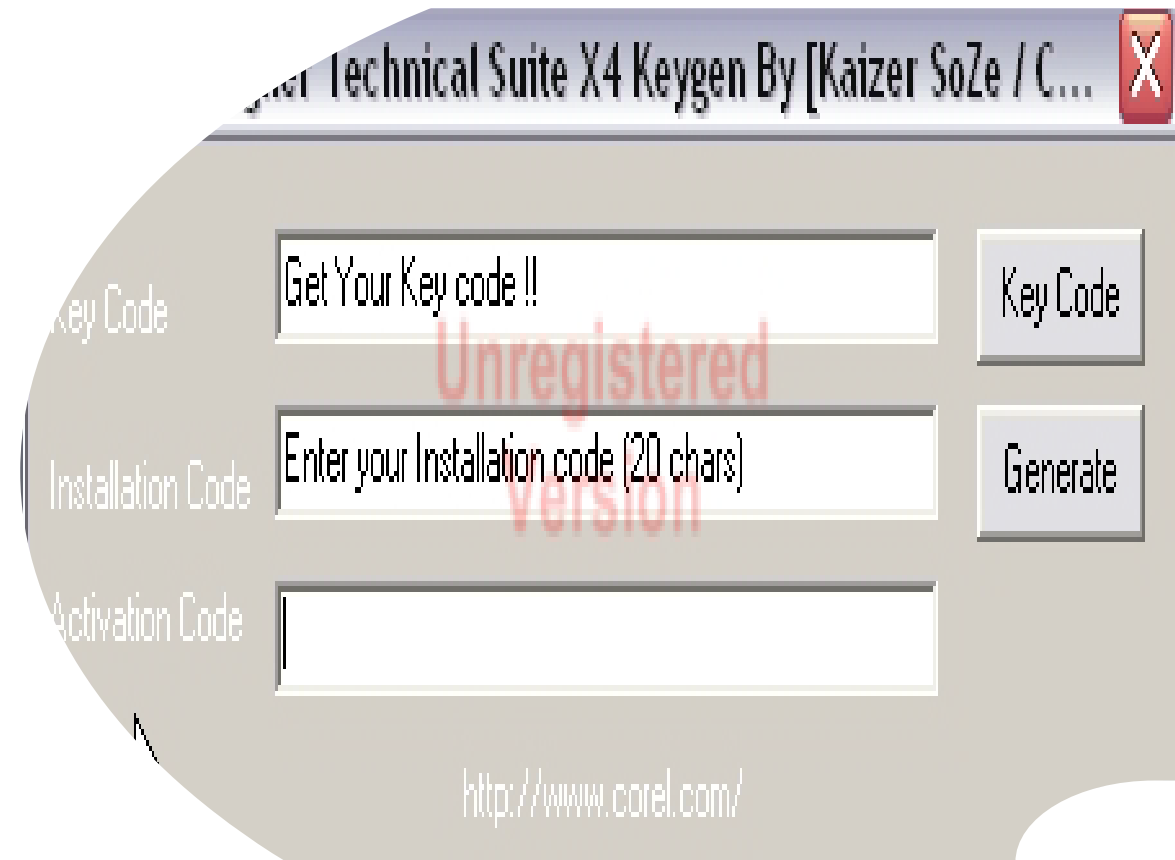


Cartoon by Maikel Nabil Sanad (Egypt, 2011)



Civil Society in the Rest of the World: the context

- Unreliable network connections
- Cracked software, poor security hygiene
- Little funding
- Trauma



Source: Wikimedia Commons



A group of people are gathered in a lush, green forest. In the foreground, a man wearing a green shirt and a backpack is speaking to a group of people. He is holding a notebook and a pen. The group consists of several individuals, including a woman in a pink shirt and a cap, and a man in a blue cap. They are all looking towards the man in the green shirt. The background is filled with dense foliage and trees.

Who am I to tell you this?



Digital Threats

So, is this where we talk about Pegasus?



Pegasus statue in Mexico City



Platform account issues

Facebook, Google

- Account takeovers

- Session hijacks

- 'Feel' like account is not theirs
two-factor authentication

- Blocks

- WhatsApp/Sign
takeovers



Thank you
Your support powers our independent journalism

The Guardian

News **Opinion** **Sport** **Culture** **Lifestyle**

World UK Coronavirus Climate crisis Environment Science Global development Football

Twitter

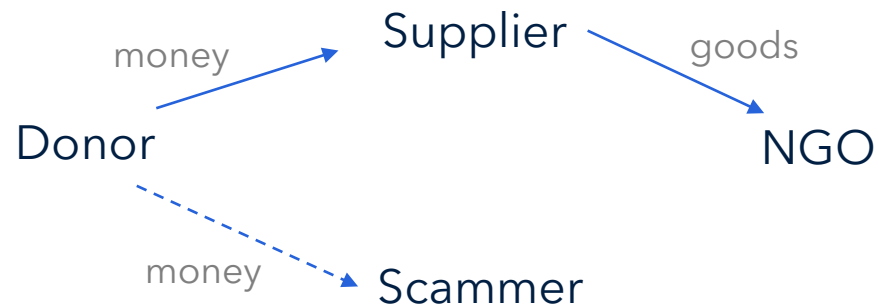
🕒 This article is more than **2 months old**

Twitter suspends accounts of several journalists who had reported on Elon Musk

Many at CNN, Washington Post and the New York Times who had written critically of the new owner found their handles suspended



BEC scam targeting small NGO



- NGO's Yahoo account got hacked
- Emails from donor filtered from inbox
- Fake emails from domain similar to supplier's sent to NGO (maybe manually moved from spam?)

Properties

Custom Details Previous Versions

Value

Description

Object

Tags

Categories

Comments

Origin

Authors csrhearmore

Last saved by carty tradings

Revision number 6

Version number

Program name Microsoft Office Word

Company

Manager

Document created 12/29/2017 12:10 PM

Document saved 10/15/2022 12:38 AM

Document time 00:25:00



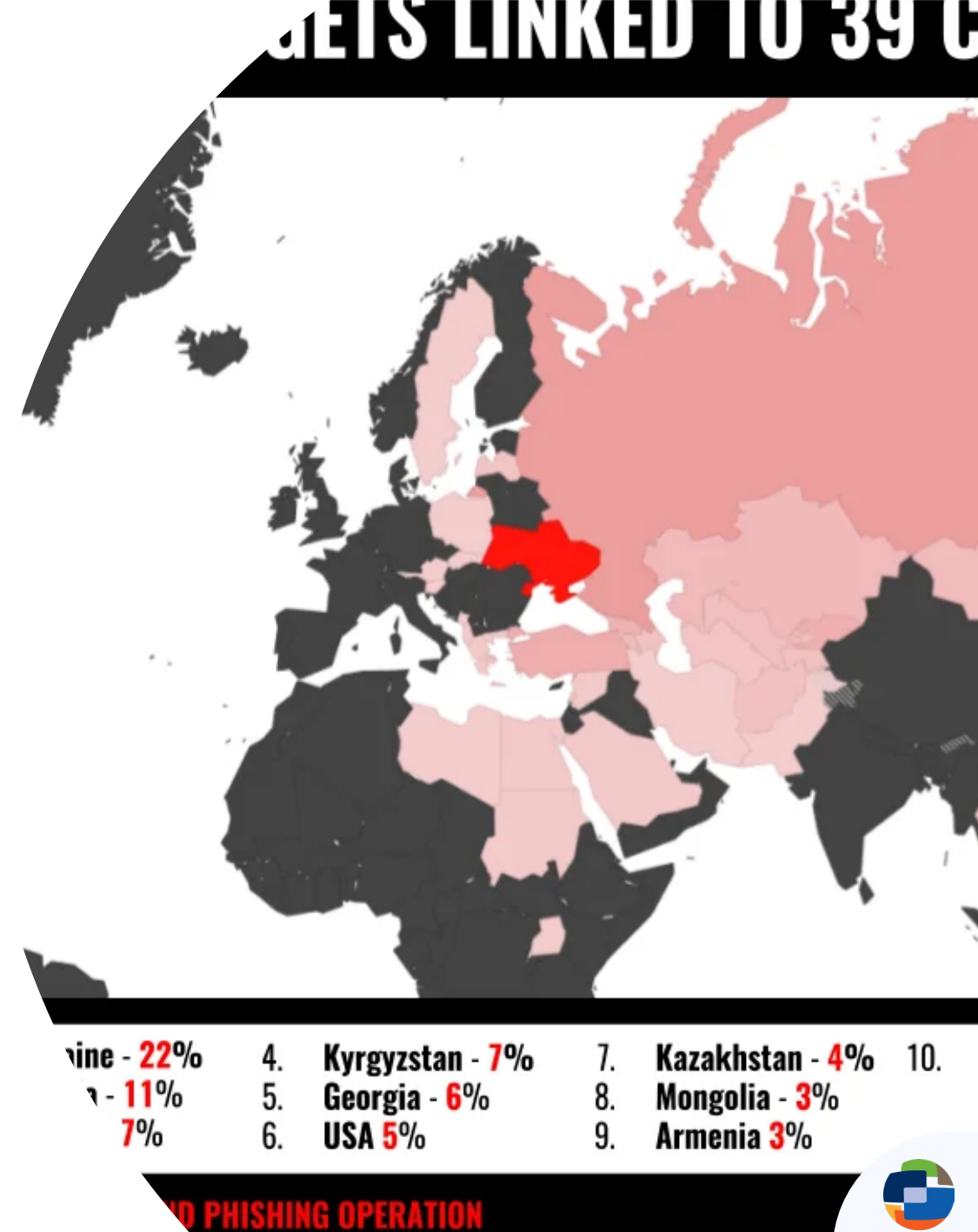
Mustang Panda

- “Interests aligned with the government of China”
- Also known as Earth Preta
 - Nick Dai’s Botconf talk at 14:50 on Thu!
- Uses PlugX, Cobalt Strike
- Often uses DLL hijacking
- Broad targeting, not very advanced
- Targets include governments, NGOs, media orgs
- But what to do if you’re targeted?



Tainted leaks

- Documents stolen through phishing, then **manipulated** and leaked
- Known to have been used by Fancy Bear/APT28 against journalists
- Source: Citizen Lab 2017
<https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/>



Transnational repression

- Targeting of civil society diaspora community
- Known actors include Iran, Syria, Egypt, Ethiopia, China
- Paper: "Psychological and Emotional War: Digital Transnational Repression in Canada"

[https://citizenlab.ca/wp-](https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf)

[content/uploads/2022/03/Report151-](https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf)

[dtr_022822.pdf](https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf)



Mercenary actors (hackers-for-hire)

- Hired by governments, sometimes private companies
- From script kiddy-level to very advanced
- Links with cybercrime and/or government
- Makes hacking and spyware available at any level to any actor
- Civil Society common targets



Our Approach

Our deep industry knowledge coupled with our close partnerships with clients enable us to bring fresh perspectives and creative thinking to the problems we solve. Our entrepreneurial spirit drives us to discover better



Mission & Vision

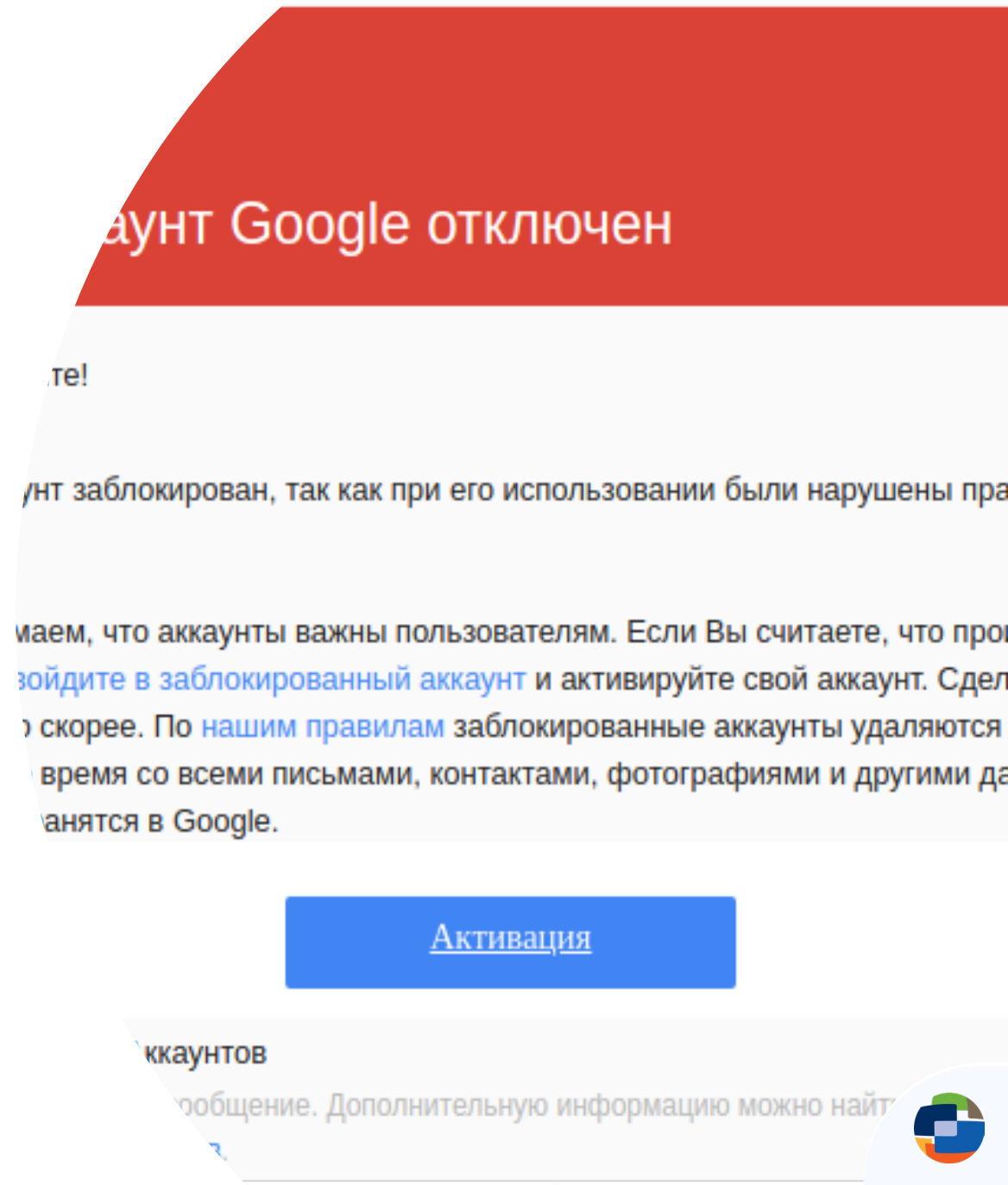
To attain global best practices and become a leading consulting company. To be an internationally respected consultant offering comprehensive solutions.

[read more -](#)



Mercenary actors: examples

- Environmental activist groups targeted by Dark Basin (BellTrox)
- Mexican journalists targeted by Hacking Team
- Togolese activists targeted with Donot spyware
- Uzbekistan civil society targeted with phishing, spyware
- Pegasus!



Use of 'revenge porn' against dissidents

- Intimate photos, audio recordings published of Azerbaijani activists
- Possibly obtained through spyware
- Source: OCCRP 2023

<https://www.occrp.org/en/37->

[ccblog/ccblog/17486-how-revenge-porn-is-used-to-silence-dissidents-in-azerbaijan](https://www.occrp.org/en/37-ccblog/ccblog/17486-how-revenge-porn-is-used-to-silence-dissidents-in-azerbaijan)



Team Jorge

- Disinformation linked with account hacks, possibly spyware
- TTPs very unclear, most knowledge based on leaked “marketing claims”
- OCCRP case study:
<https://www.occrp.org/en/storykillers/israeli-disinformation-expert-linked-to-faked-bank-accounts-in-serbian-smear-campaign>



Pegasus

- Developed by NSO Group
- Uses zero-day, zero-click exploits on iPhones
- We don't know much about other devices, including Android
- Civil society targeted around the world
- Very hard to defend against
- Pegasus or Pegasus suspicion can be extremely traumatizing



Incident response

- Limited telemetry and logs
- EDR/MDR hard to do in a sustainable way
- Targets often want to move on quickly
- Trauma often leads to extreme distrust
(sometimes: extreme trust), hypervigilance,
“unreliable narrators”



How can you help

- Reverse engineering?
- Threat sharing (both ways!)
 - TTPs preferable over IOCs
- Product and platform licenses
- Training
- Research collaboration
- **Funding!**



Thank you! Questions?

mgrooten@internews.eu

Ask for Signal, etc.

