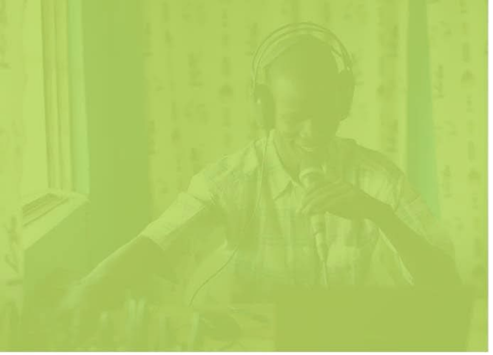
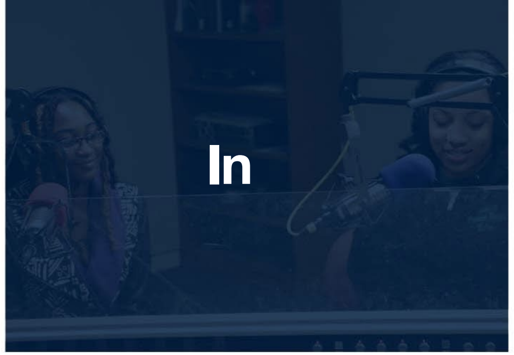
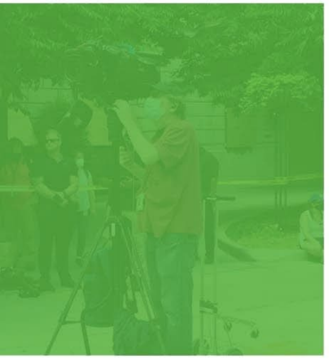


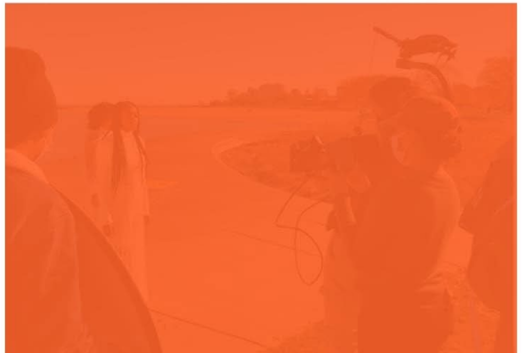


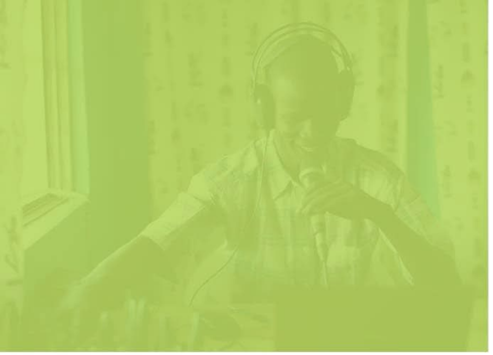
Digital threats against civil society in the rest of the world

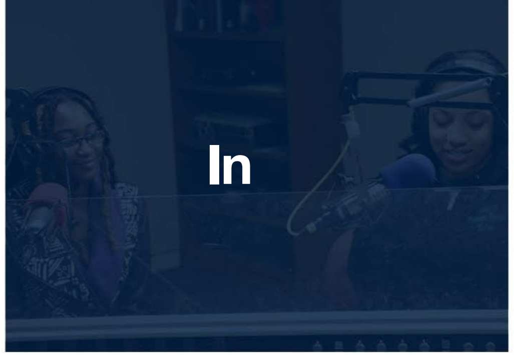
Martijn Grooten, Internews

Botconf 2023, Strasbourg, France

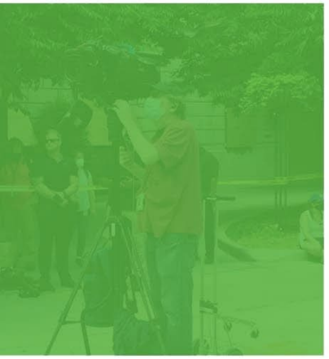








In



Digital threats against civil society in the rest of the world

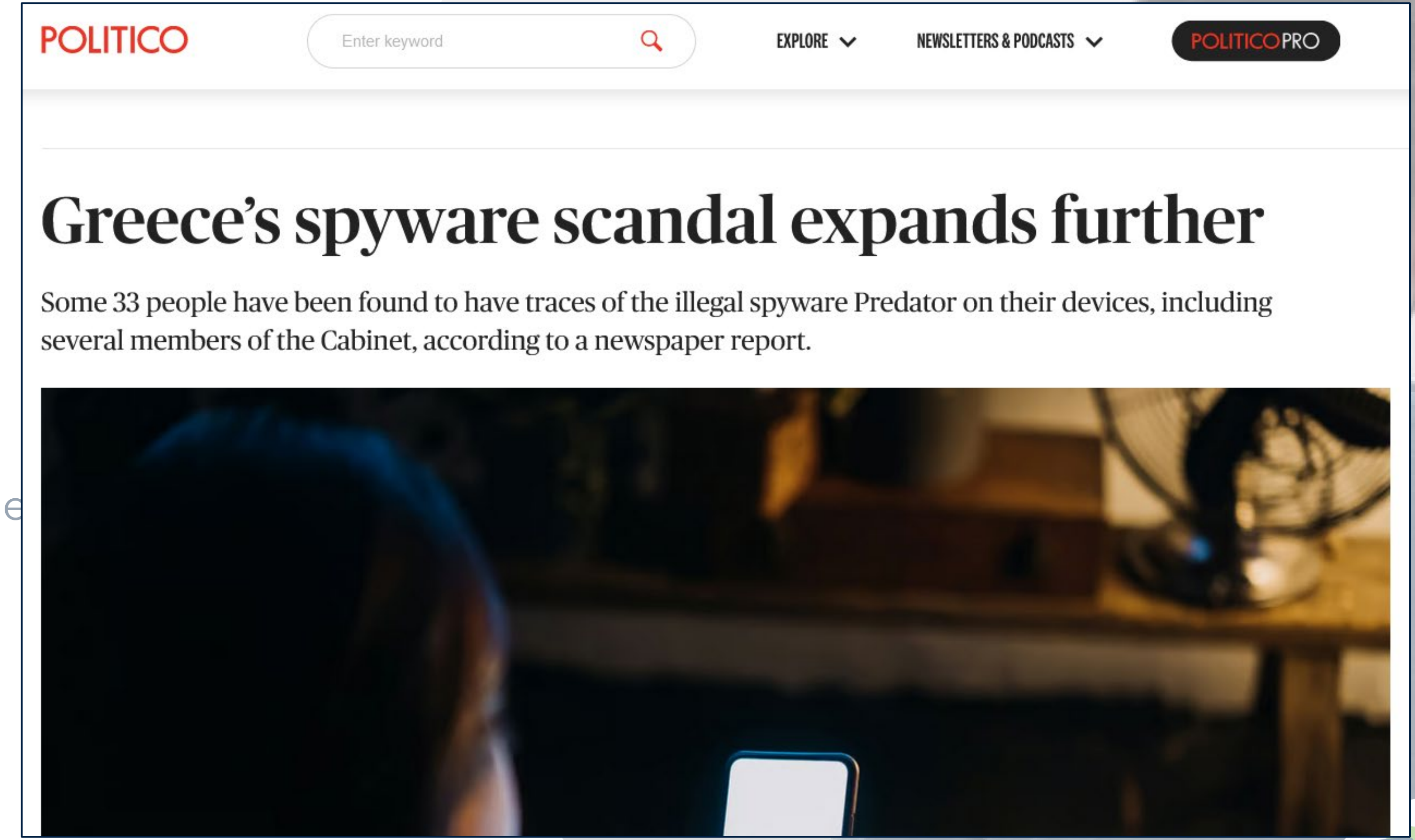
Martijn Grooten, Internews

Botconf 2023, Strasbourg, France

TLP:WHITE

About me

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



Greece's spyware scandal expands further

Some 33 people have been found to have traces of the illegal spyware Predator on their devices, including several members of the Cabinet, according to a newspaper report.

Internews

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”

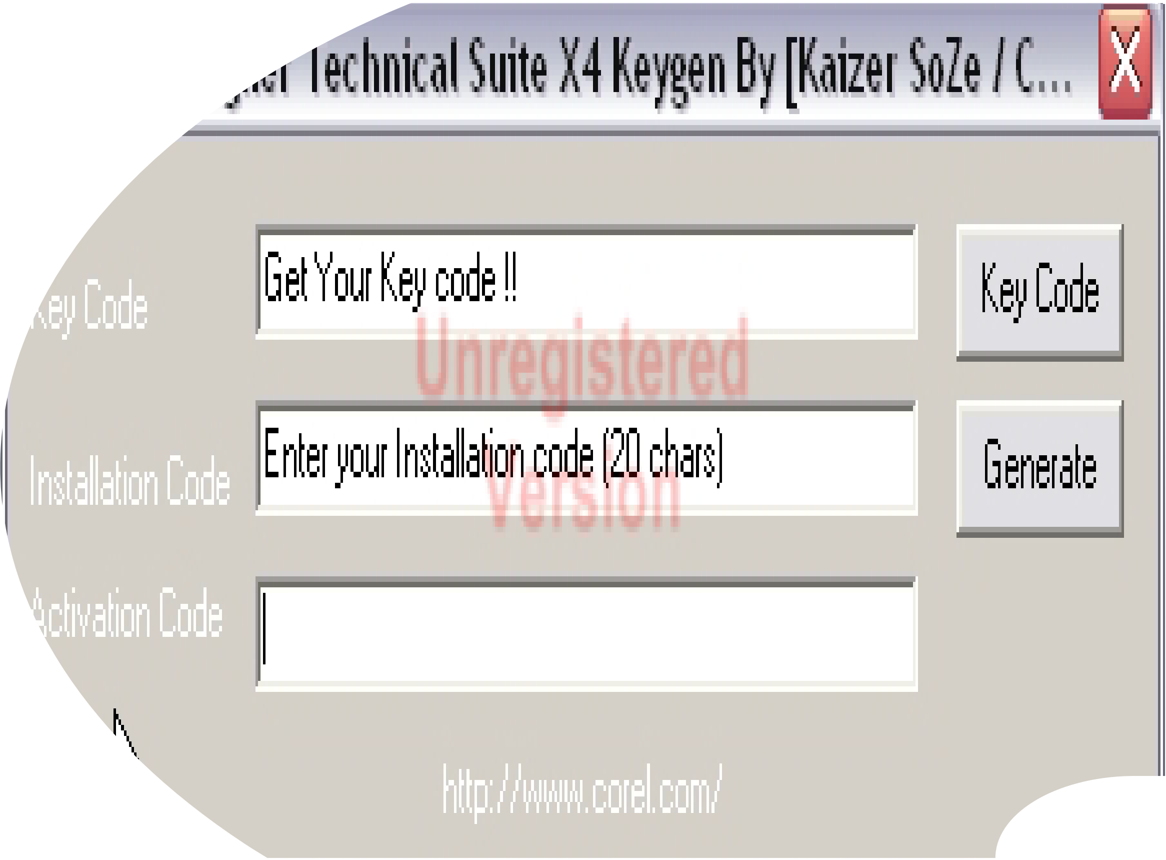
Civil Society in the Rest of the World: the context

- 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



Technical Suite X4 Keygen By [Kaizer SoZe / C...

ey Code: Get Your Key code !!

Installation Code: Enter your Installation code (20 chars)

ctivation Code:

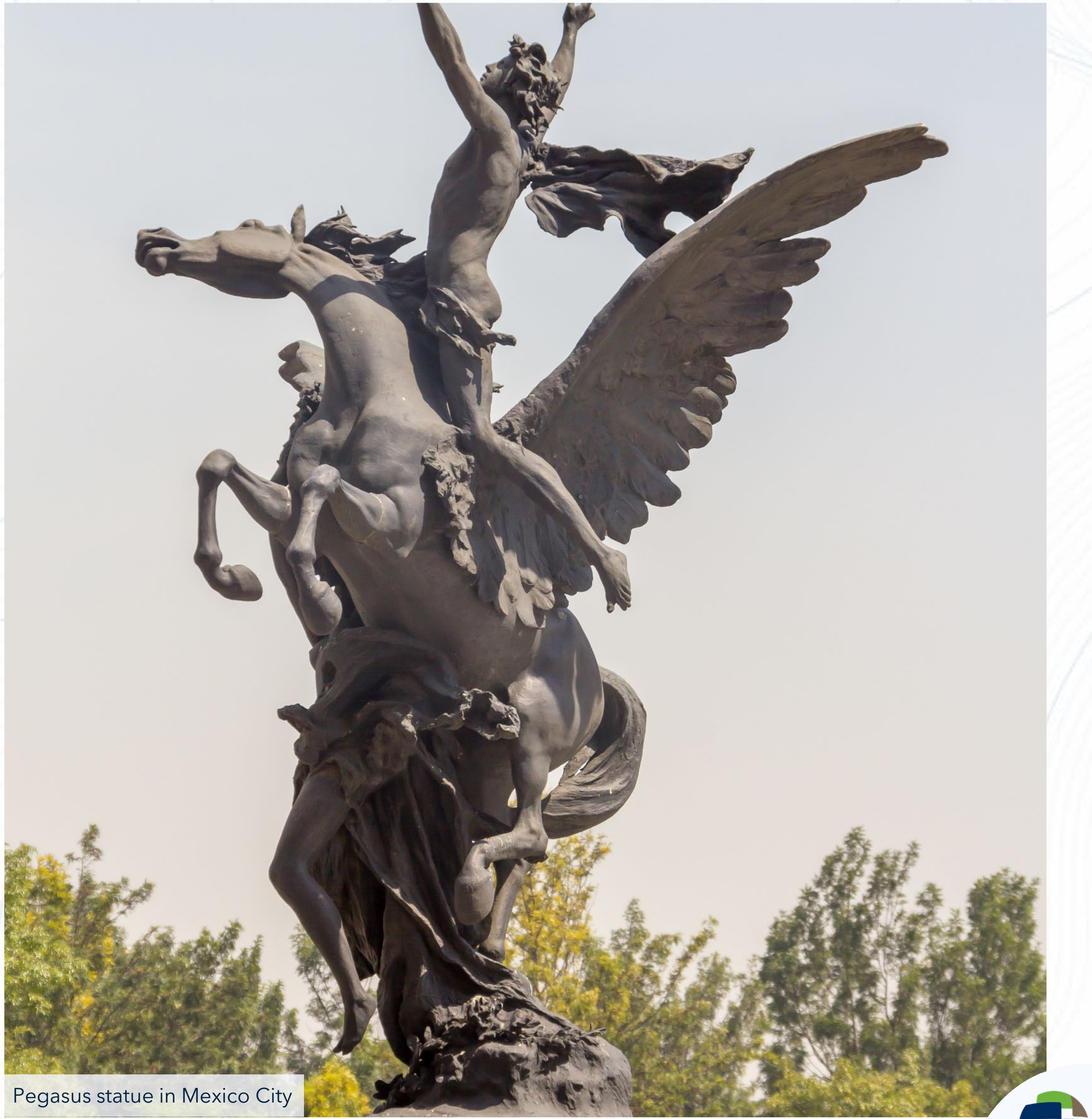
http://www.corel.com/

Source: Wikimedia Commons

Who am I to tell you this?

Digital Threats

So, is this where we talk about Pegasus?

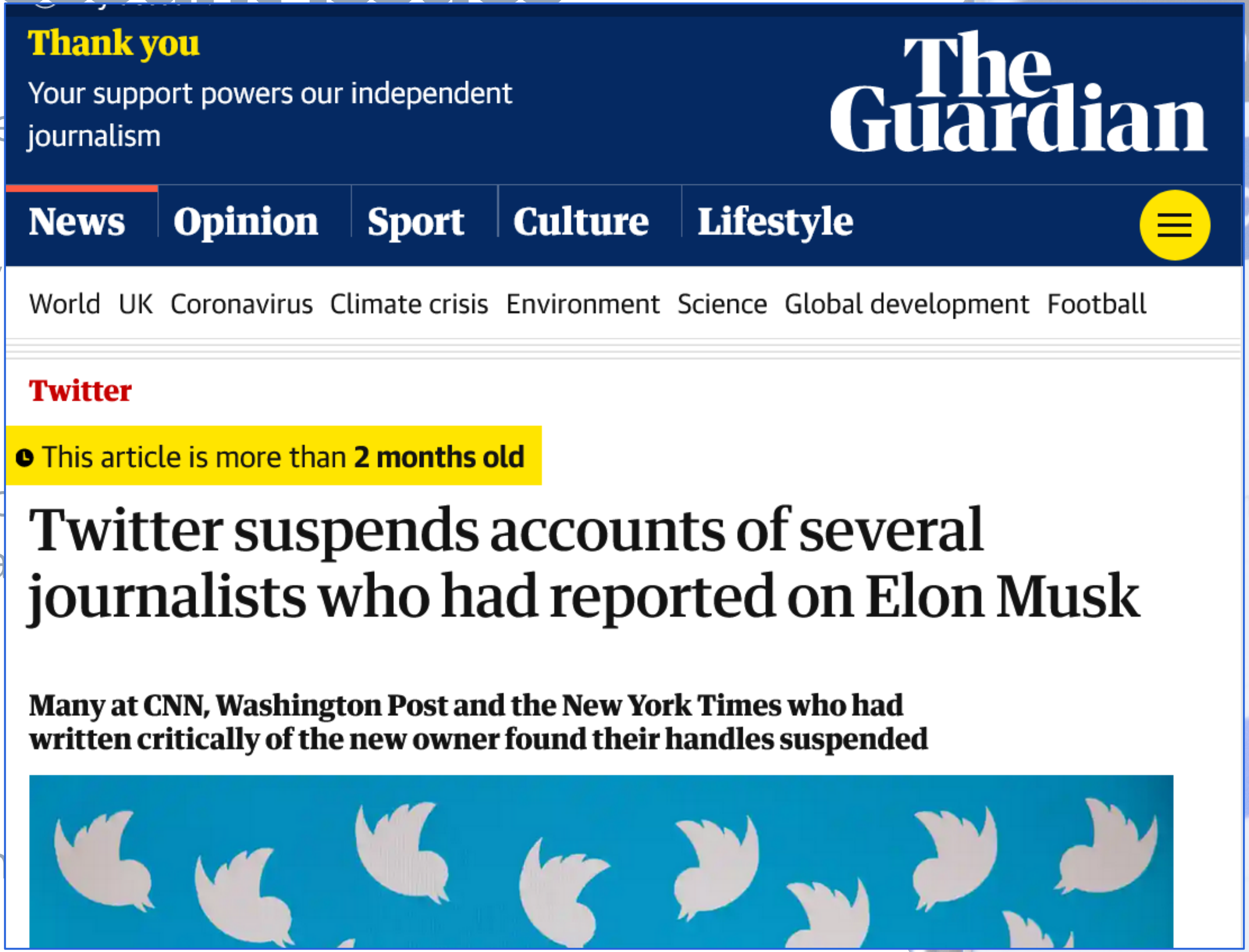


Pegasus statue in Mexico City

Platform account issues

Facebook, Google

- Account takeov
- Session hijacks
  - ‘Feel’ like ac two-factor a
- Blocks
- WhatsApp/Sign takeovers



Thank you

Your support powers our independent journalism

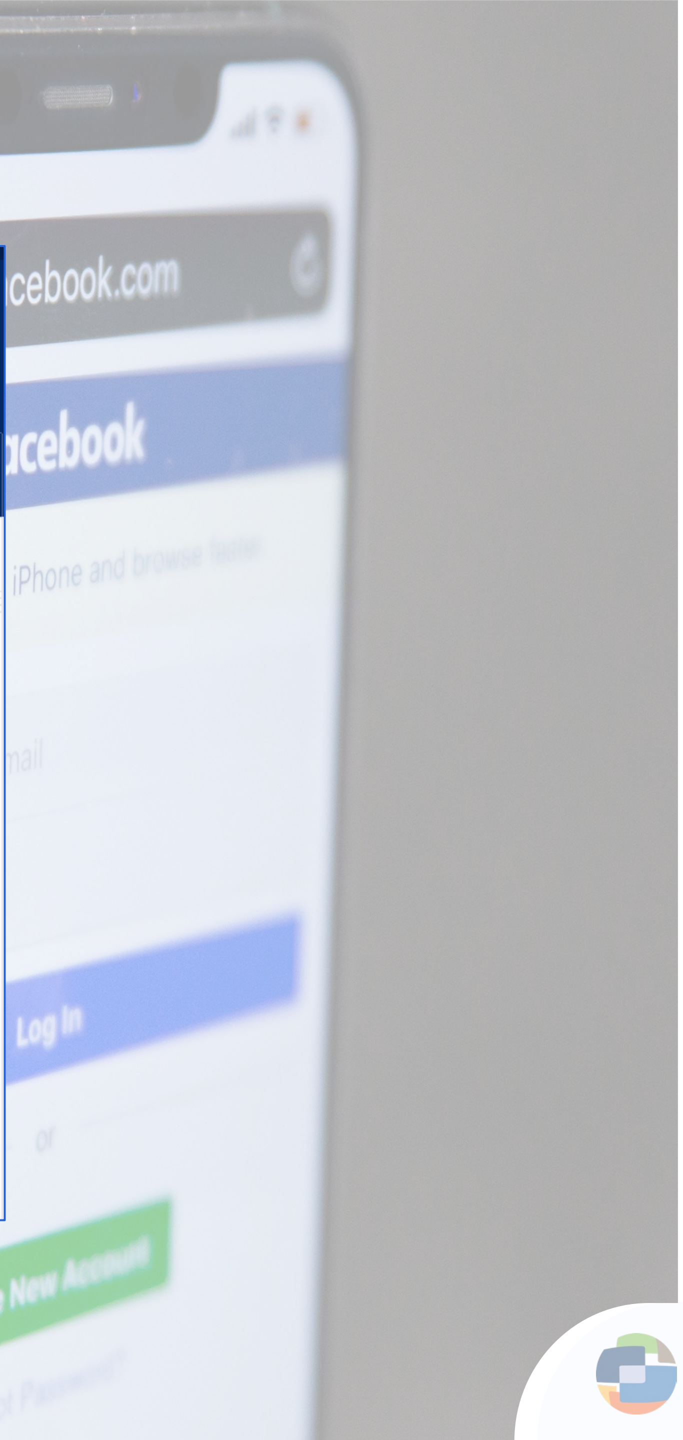
The Guardian

Twitter

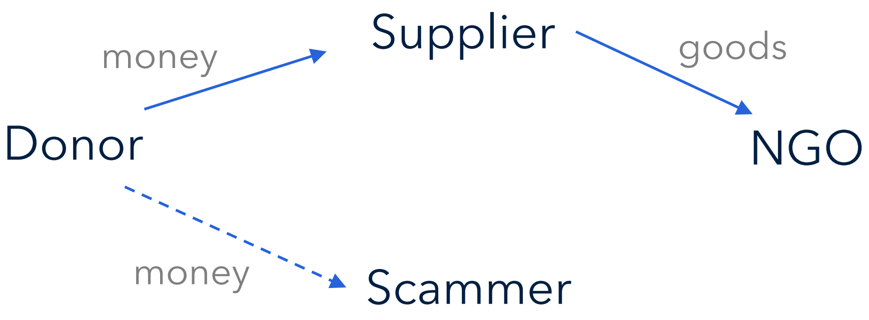
This article is more than **2 months old**

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

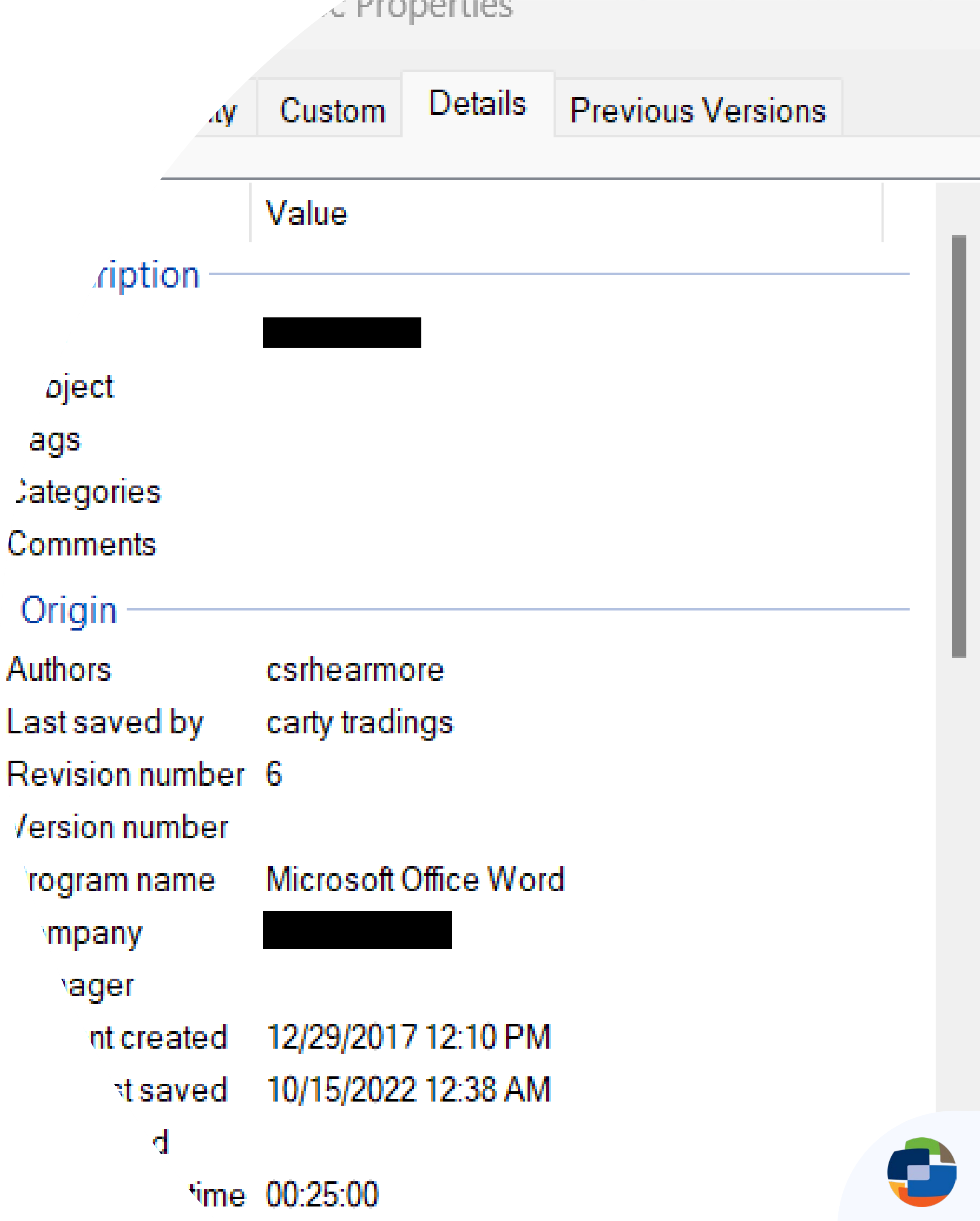
Many at CNN, Washington Post and the New York Times who had written critically of the new owner found their handles suspended



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?)



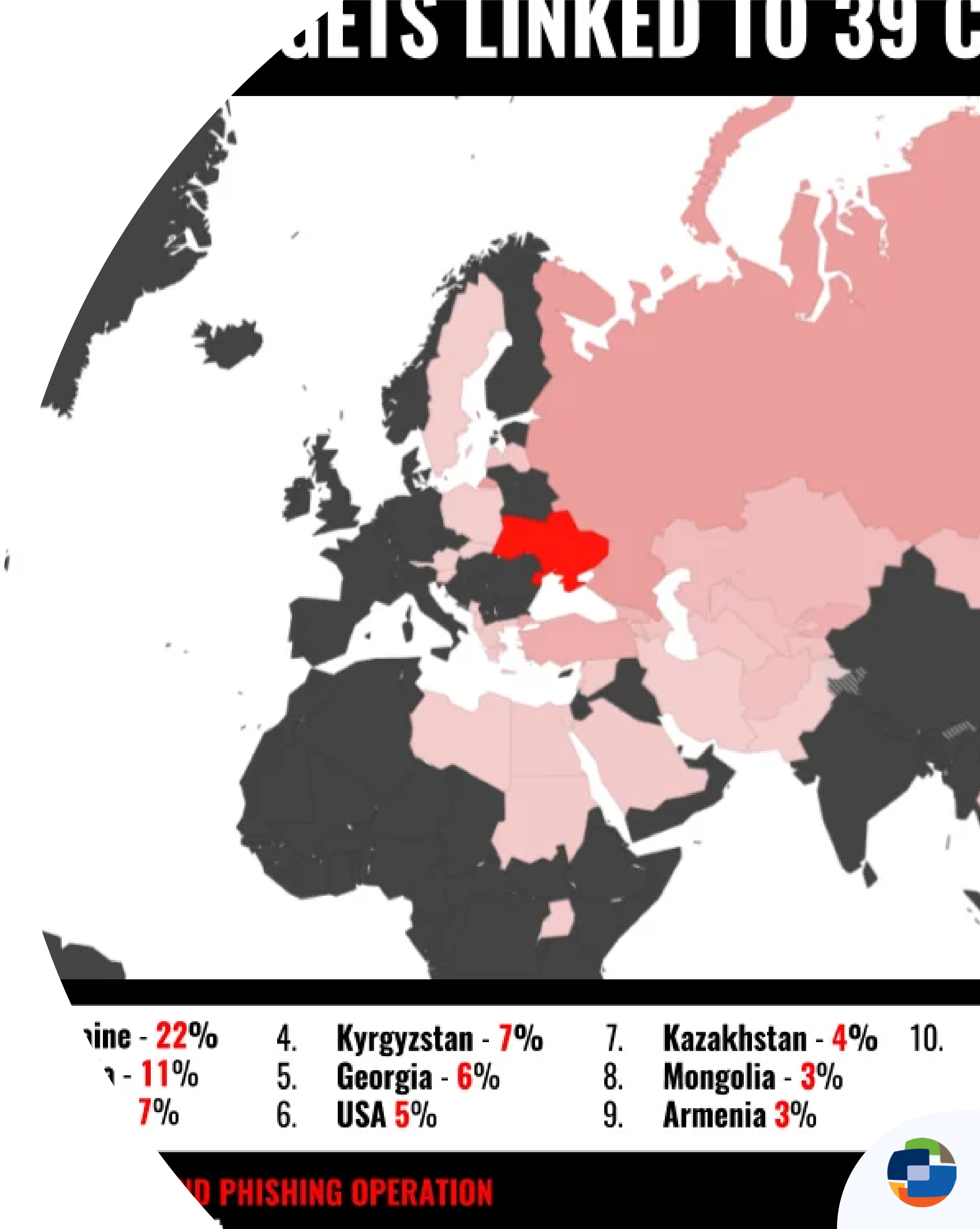
	Value
ription	
	[redacted]
oject	
ags	
ategories	
Comments	
Origin	
Authors	csrhearmore
Last saved by	carty tradings
Revision number	6
ersion number	
rogram name	Microsoft Office Word
mpany	[redacted]
ager	
nt created	12/29/2017 12:10 PM
t saved	10/15/2022 12:38 AM
d	
ime	00:25:00

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?

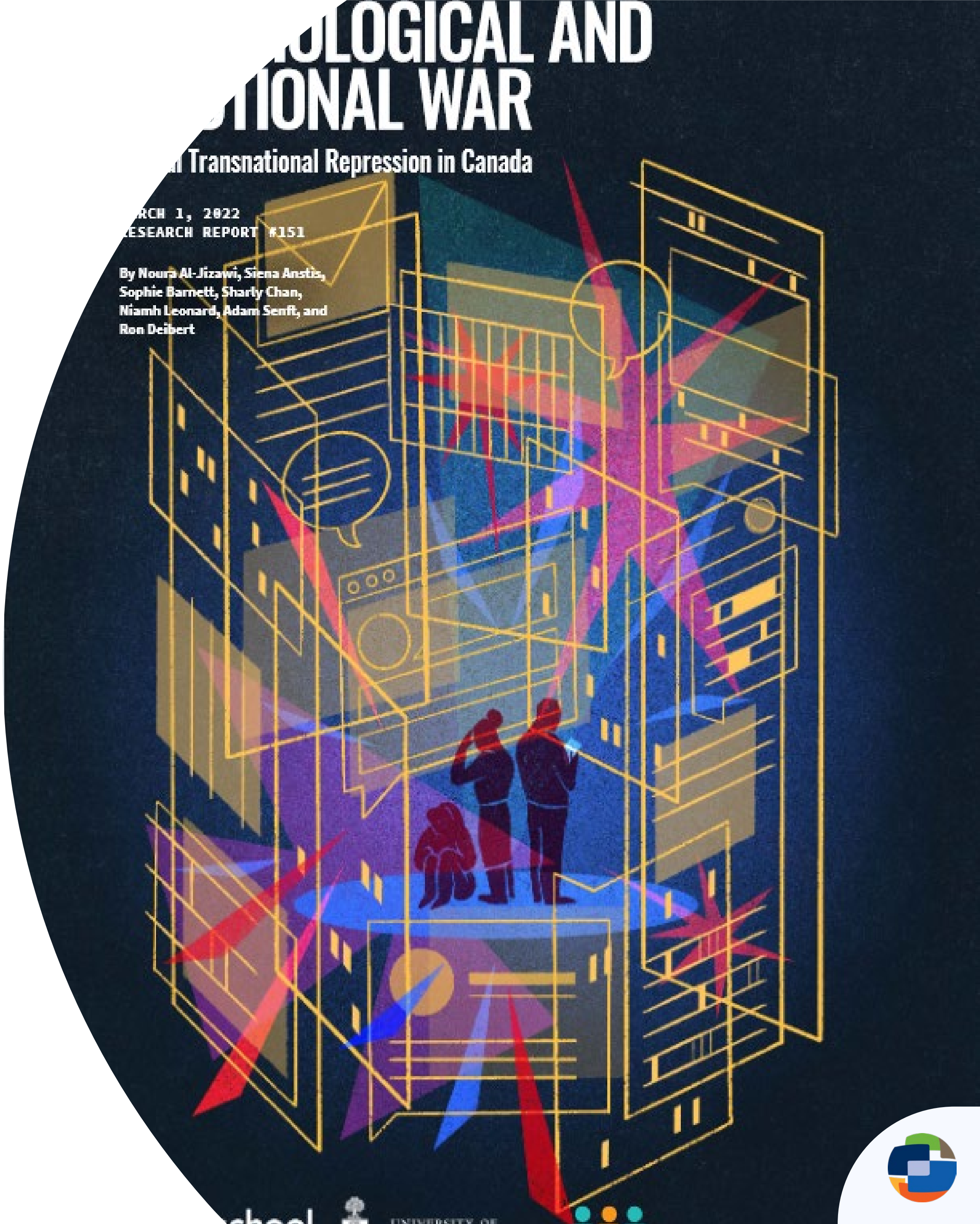
Tainted leaks

- 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

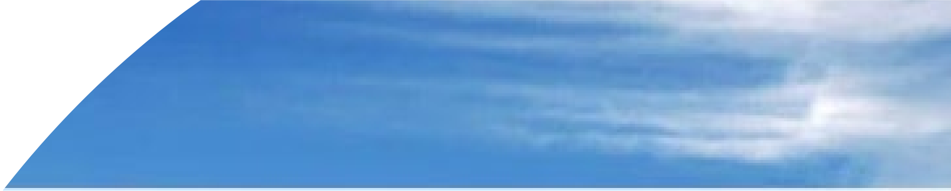
- Targeting of civil society diaspora community
- Known actors include Iran, Syria, Egypt, Ethiopia, China
- Paper: “Psychological and Emotional War: Digital Transnational Repression in Canada” https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf



OLOGICAL AND
TIONAL WAR
l Transnational Repression in Canada

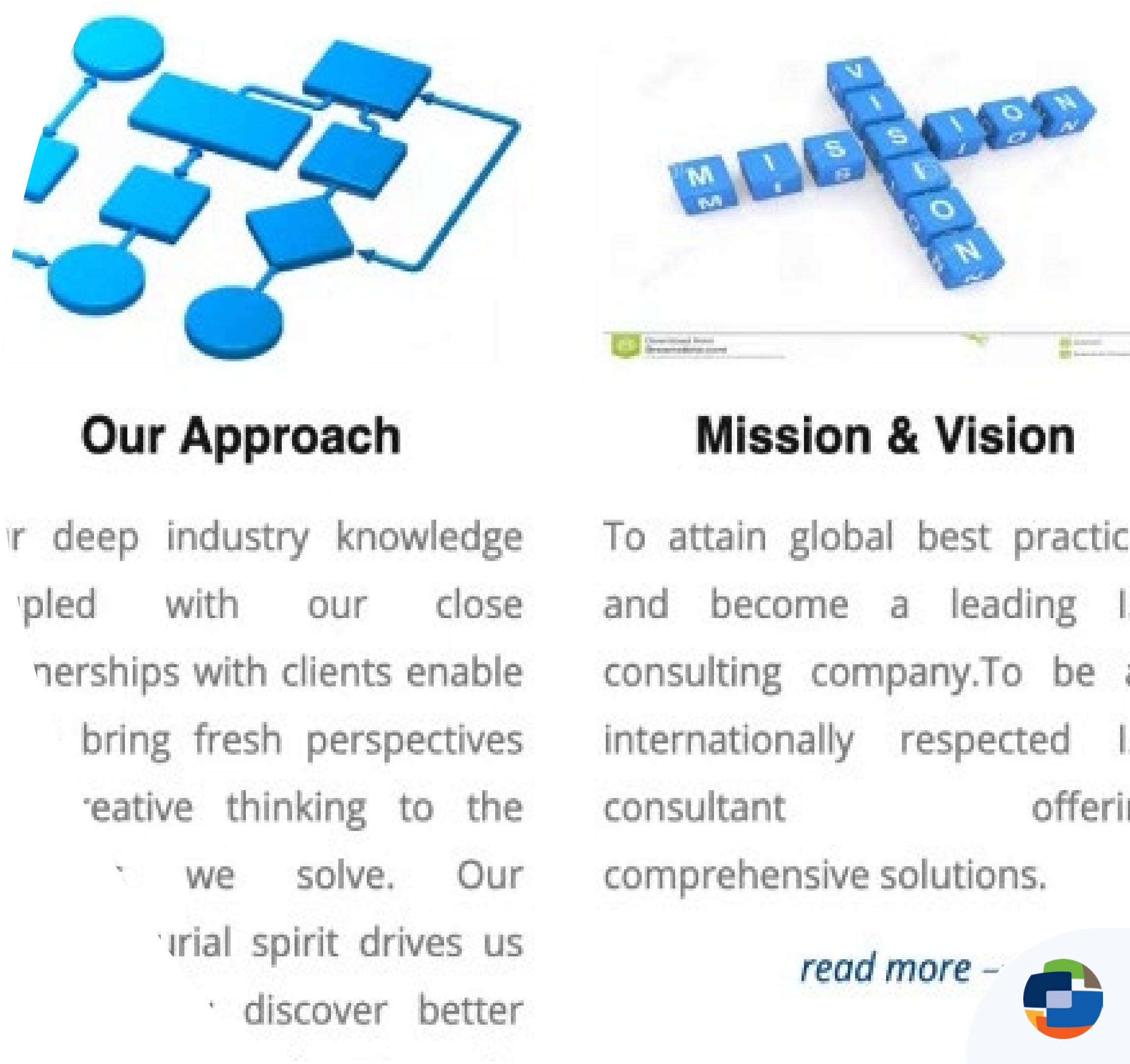
RCH 1, 2022
ESEARCH REPORT #151

By Noura Al-Jizawi, Siena Anstis,
Sophie Barnett, Sharly Chan,
Niamh Leonard, Adam Senft, and
Ron Deibert



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

r deep industry knowledge pled with our close nerships with clients enable bring fresh perspectives eative thinking to the we solve. Our rial spirit drives us discover better

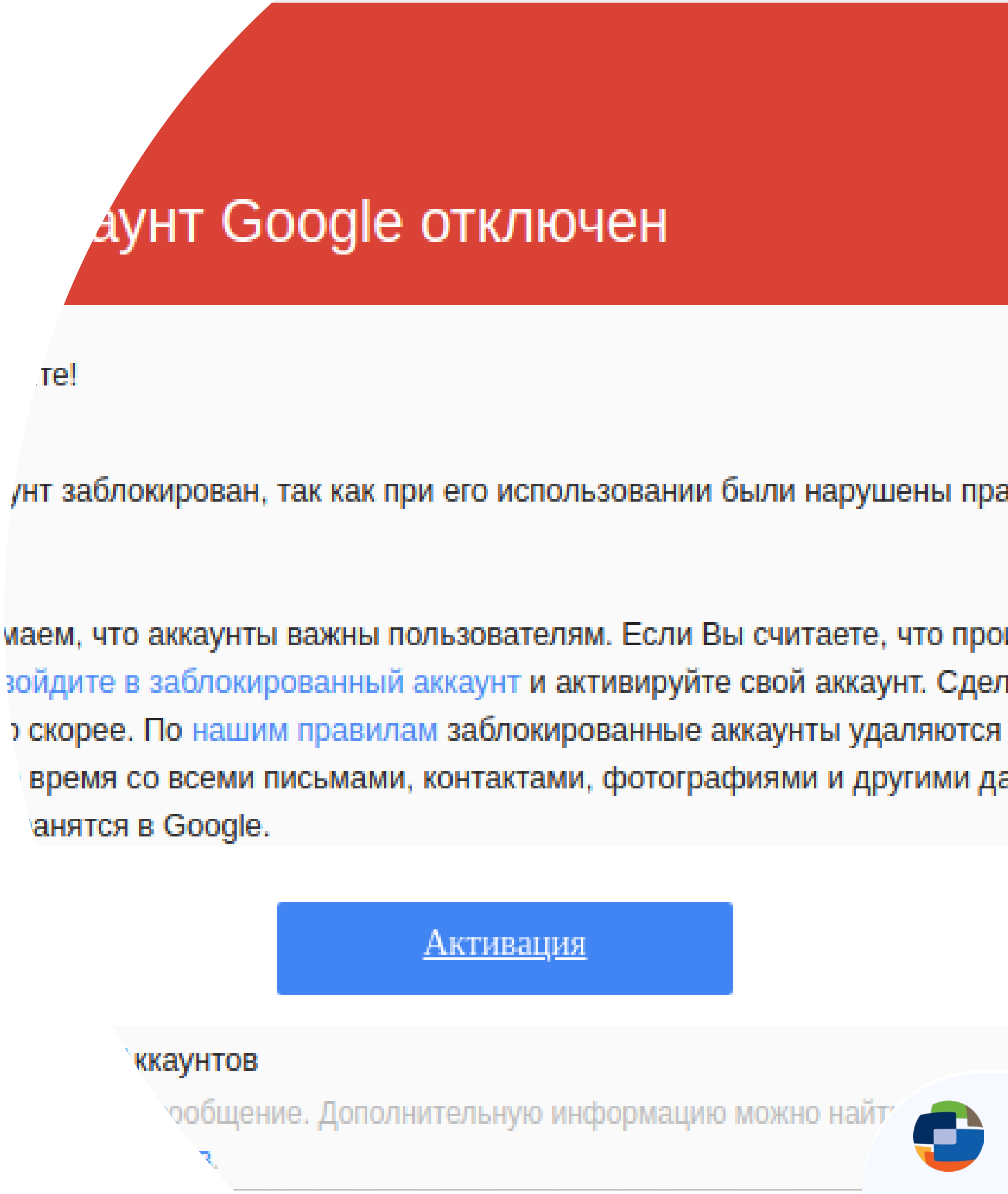
Mission & Vision

To attain global best practic and become a leading I consulting company.To be a internationally respected I consultant offeri 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!



аунт Google отключен

те!

унт заблокирован, так как при его использовании были нарушены пра

маем, что аккаунты важны пользователям. Если Вы считаете, что про
зойдите в заблокированный аккаунт и активируйте свой аккаунт. Сдел
скорее. По нашим правилам заблокированные аккаунты удаляются
время со всеми письмами, контактами, фотографиями и другими да
анятся в Google.

ккаунтов

ообщение. Дополнительную информацию можно найт

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

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.