

# THREAT MODELING & ANALYSIS

Digital Security for Journalists and Human Rights Defenders  
By Ronalyn V. Olea | Bulatlat, NUJP

# WHAT IS DIGITAL SECURITY?

The protection of one's digital or electronic identity and information

Browser cookies

Persistent logins on mobile device and web eg.

Facebook, Google

Logins on apps

IP Address + connections

Metadata in photos, documents, social media posts

Mobile tower access (~500m), calls

WiFi connections (even if not connected)

Electronic files





# WHAT ARE THE COMMON DIGITAL SECURITY ISSUES FACED BY PH JOURNALISTS & HUMAN RIGHTS DEFENDERS?

Enumerate common digital security issues/ concerns you and/or your colleagues have confronted in the past few years.



# THE RISE OF DIGITAL AUTHORITARIANISM

## *A “Natural Tool” for Autocrats*

While The Pegasus Project exposes clear cases of misuse of NSO Group’s software, the company is just one player in a global, multi-billion-dollar spyware industry.

Estimated by NSO managers to be worth approximately \$12 billion, the mobile spyware market has democratized access to cutting-edge technology for intelligence agencies and police forces that, in years past, could only dream of having it.

“You’re giving lots more regimes an intelligence service,” said John Scott-Railton, a senior researcher at Citizen Lab. “Like a foreign intelligence service in a box.”



Disinformation, attacks on credibility of human rights advocates, digital surveillance, cyber attacks, "anti-terrorism" laws

# BIGGEST ATTACKS

Case

## Three Philippine media outlets face latest in a string of cyberattacks


February 1, 2022 7:19 AM EST



Three Philippine news websites, ABS-CBN News, Rappler, and Vera Files, publicized separate distributed denial-of-service (DDoS) attacks between December 11 and 23, 2021. The attacks flood websites with requests to prevent them from functioning, and the sites were periodically forced offline by huge spikes in traffic coinciding with political news coverage.

All three sites have been openly critical of the Duterte regime. The National Union of Journalists of the Philippines released a **statement** condemning the attacks and called for an investigation.

# BIGGEST ATTACKS

The Igloo program ▾

Home » Israeli firm 'Bright Data' (Luminati Networks) enabled the attacks against Karapatan

## ISRAELI FIRM 'BRIGHT DATA' (LUMINATI NETWORKS) ENABLED THE ATTACKS AGAINST KARAPATAN

in Alerts / Philippines tagged DDoS

Stockholm, August 25th, 2021

The 25 days long DDoS attack against the website of [Karapatan](#) was launched by almost 30.000 IP addresses, whereas one third of the addresses originated from devices that there were not running "Open Proxies" or "Tor exits". Identifying this mysterious part of the botnet turned to be a fascinating research and a digital forensics challenge. The traces lead us to an Israeli firm offering access to millions of proxies in mobile operators, data centers and residential buildings – a perfect infrastructure to hide the source of DDoS attacks.


This is Part II of our ongoing research on the DDoS attack against Karapatan. For background information, please read the report "[Human rights alliance 'Karapatan' under long lasting DDoS attack](#)".

## Cyberattacks on red-tagged news sites traced to DOST, Army


By: [Krixia Subingsubing](#) - Reporter / @KrixiasINQ Philippine Daily Inquirer / 05:30 AM June 24, 2021




EDITORS' PICKMOST READ




NEWSINFO  
House energy committee chair Arroyo bats for cheap electricity




NEWSINFO  
House OKs proposed P5.268-T 2023 budget on 3rd reading



NEWSINFO  
Minority calls out huge confidential funds in 2023 budget



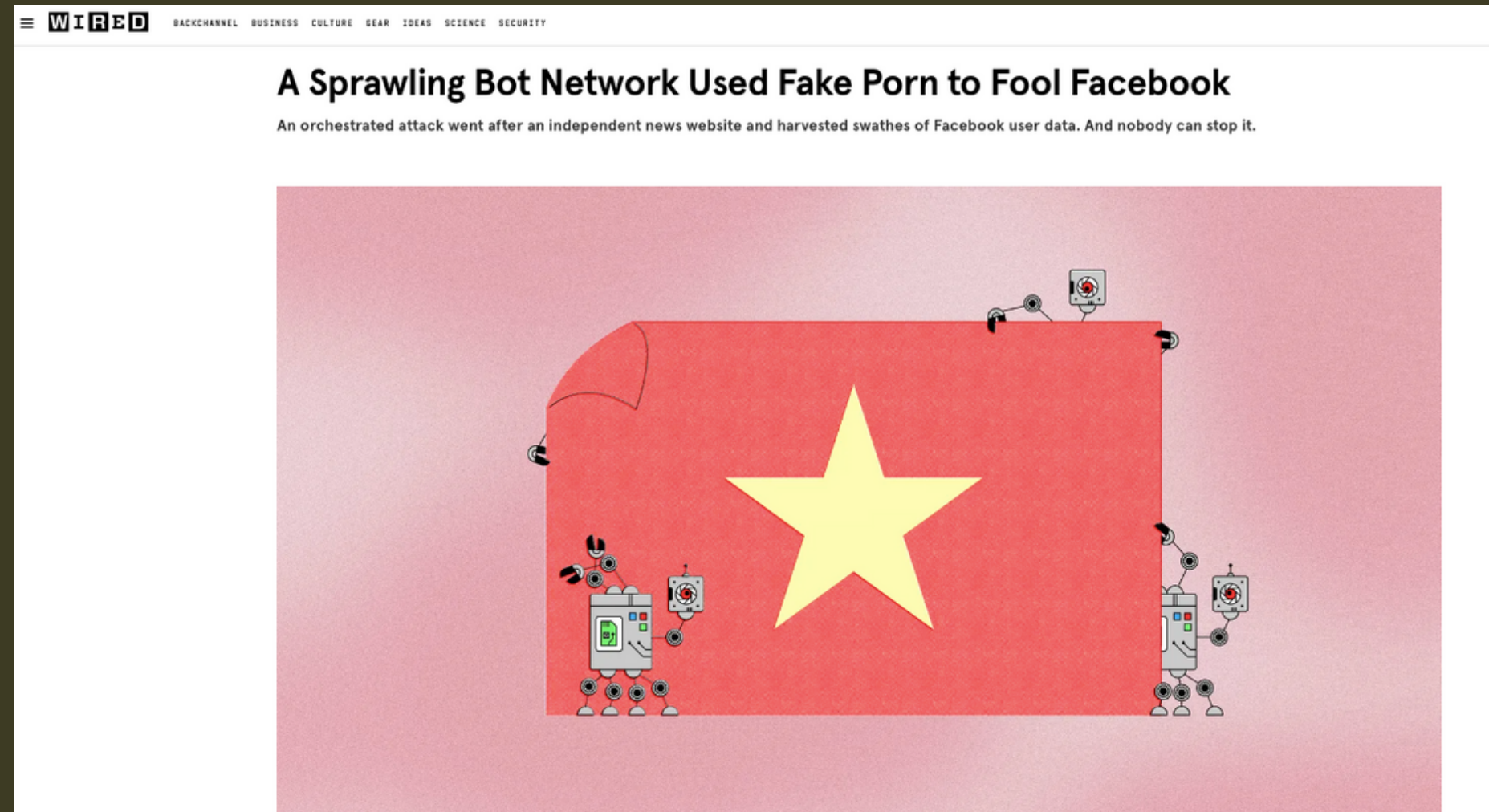
BUSINESS  
UNFPA Philippines Career Opportunities



NEWSINFO  
Key minority solons say 'yes with reservations' to




# BIGGEST ATTACKS



The volume of this attack was staggering even for Bulatlat, which has long been the target of ensorship and major cyberattacks. The team at Qurium was blocking up to 60,000 IP addresses a day from accessing Bulatlat's website. "We didn't know where it was coming from, why people were going to these specific parts of the Bulatlat website," says Lundström.

# BIGGEST ATTACKS



NEWS

Filtered By: Topstories

## Media org asks QC court to junk NTC order blocking access to its website

By LLANESCA T. PANTI, GMA News  
Published July 8, 2022 5:04pm

Alipato Media Center, Inc. on Friday asked the Quezon City Regional Trial Court to junk National Telecommunications (NTC)'s memorandum ordering internet service providers (ISP) to [block access](#) to Bulatlat.com.

Alipato Media Center, Inc. said the NTC memorandum, issued on June 8 upon the request of then National Security Adviser Hermogenes Esperon, is illegal and violates due process.

"The issuance by the NTC of its 08 June 2022 Memorandum is ultra vires. Nothing, express or implied, in EO No. 546 dated 23 July 1979, the instrument creating the NTC, and RA 7925 dated 01 March 1995 or the "Public Telecommunications Policy Act of the Philippines," which designated it as the principal administrator of the mentioned statute, clothes the NTC with the power to block the websites listed in the said Memorandum, including Bulatlat.com, without securing a court order," the complainant said.

ABS-CBN NEWS

Share



## Bulatlat says no due process before blocking of website, eyes legal action

Benise Balaoing, ABS-CBN News  
Posted at Jun 23 2022 01:27 PM







## THREAT MODELING

When it comes to the protection of your information sources and the data you already collected, it is paramount to be clear who your adversary is. Depending on the individual or the organization you are dealing with, their capabilities and willingness varies. Therefore, the tools and practices must match your adversary.

# UNDERSTAND THE CONTEXT AND WORK ENVIRONMENT

What is the situation of press freedom/human rights  
work in the country?

What kind of work environment do you have?

What kind of stories do you pursue?

Who are your usual sources?

# WHO IS WILLING TO HARM YOU?

Determine what kind of adversary you are facing. Is it an individual, a group of people, a full organization ?



# WHAT ARE THEY AFTER?

What kind of information could be of interest to them, and what would their goal be in acquiring this information?

# WHAT CAN THEY DO?

What are the technical, financial and human resources of your opponent? An isolated adversary doesn't have the same capabilities as a group.

**WHAT CAN YOU  
DO ABOUT IT?**

What can you do to mitigate  
this risk/scenario?



Scenario 1: Joining a fact-finding mission in areas with recent cases of extrajudicial killings

## Scenario 2: Covering a land dispute with armed guards, police/military deployment

[illegible]