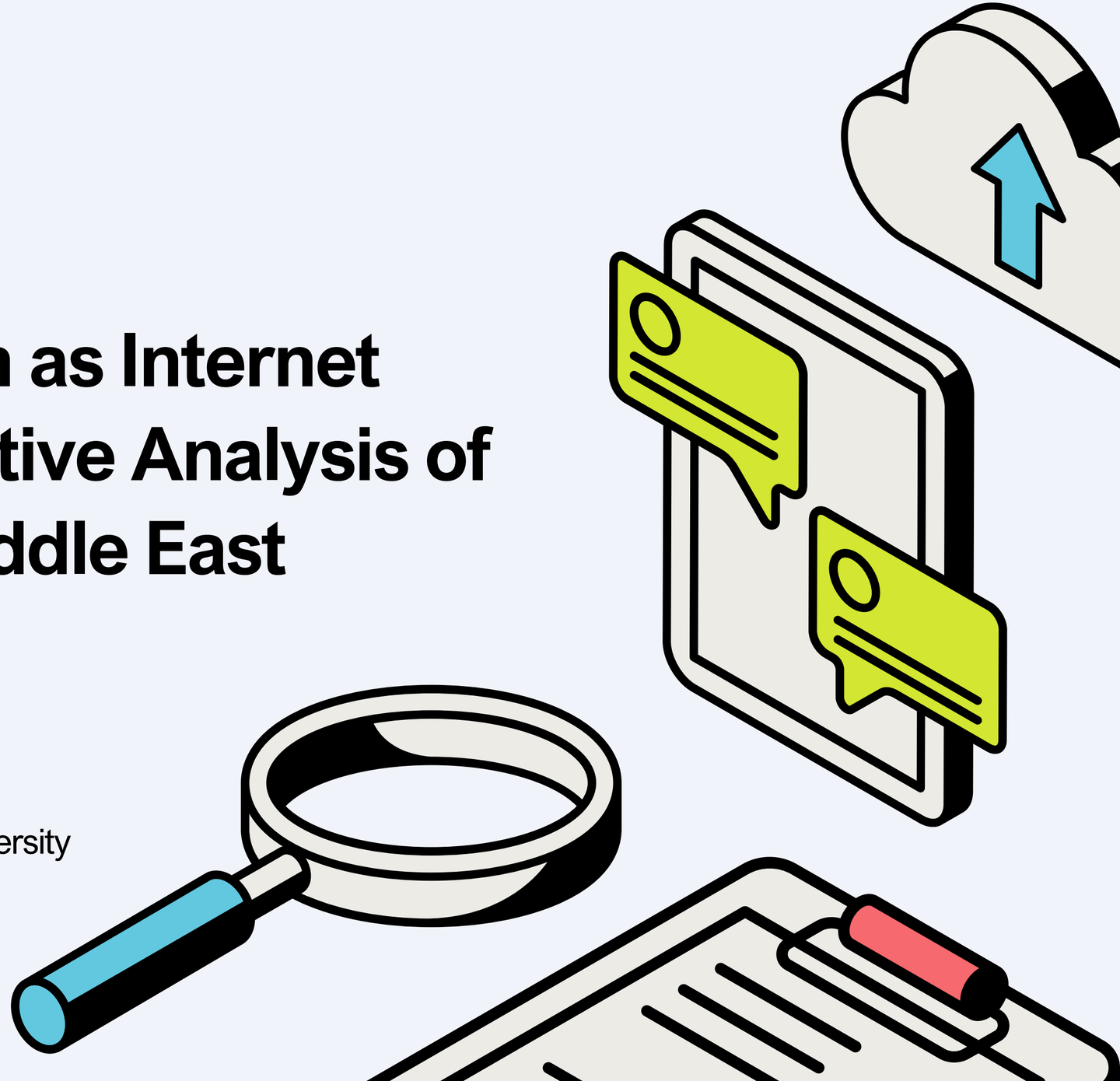
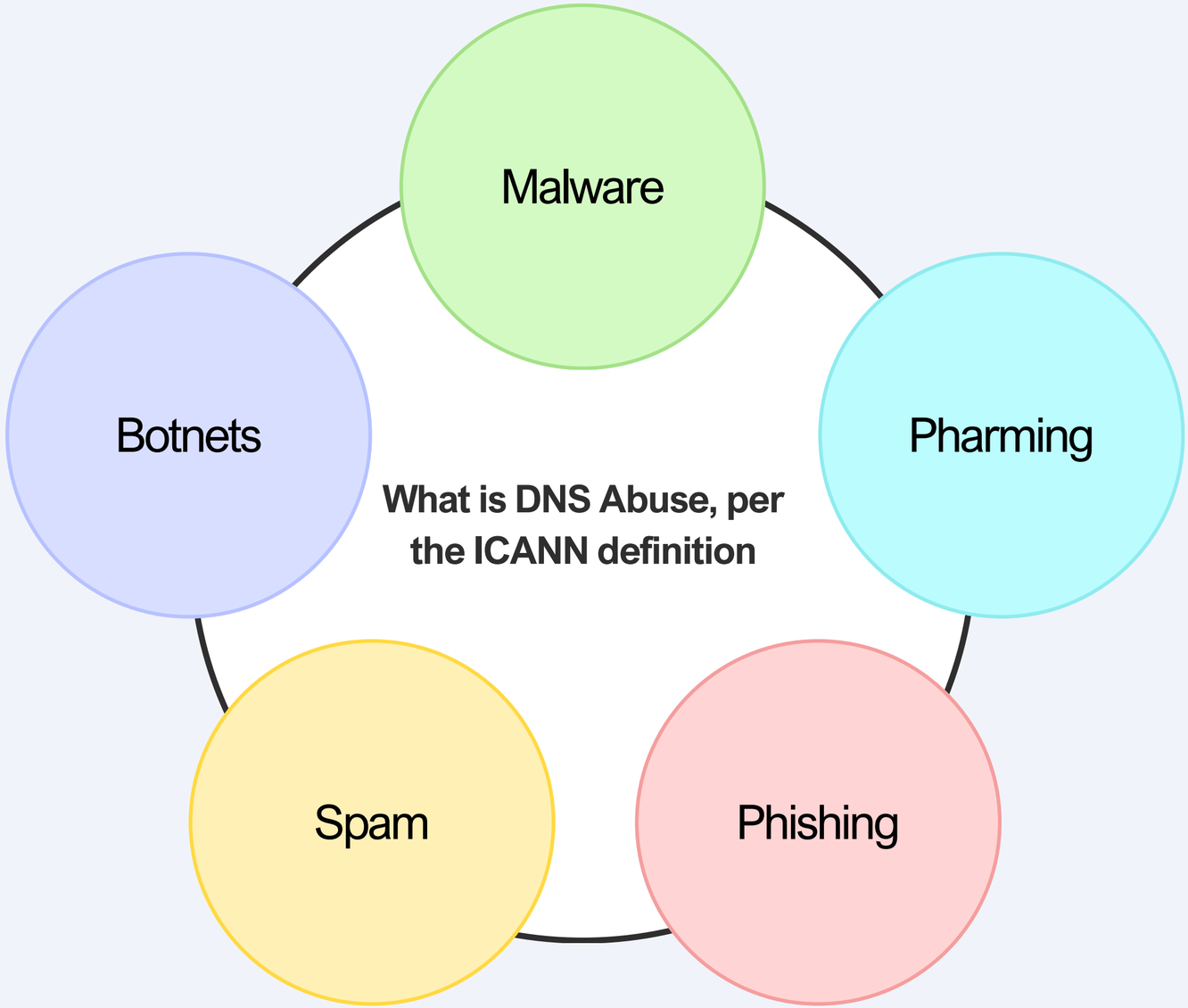
DNS Abuse Mitigation as Internet Governance: A Comparative Analysis of Europe and the Middle East

Rym Badran
European Master in Law, Data, and AI - Dublin City University
ICANN86 NextGen





Internet Corporation for Assigned Names and Numbers. DNS Abuse Mitigation Program.https://www.icann.org/dnsabuse

Why a comparison between Europe and the MENA?

Comparative table on the State of DNS Abuse in Europe and the MENA Region

Europe

European country-code Top-Level Domains, are widely reported as among the least abused TLD groups

2022 European Commission Study

Regulation Driven

EU's Cybersecurity Framework, NIS2 Directive, DSA, GDPR

More institutionalized cooperation between actors

DNS4EU Initiative

Commercially motivated

Online fraud, brand impersonation, and consumer scams. These harms usually target users, businesses, banks, for financial gain

MENA

No equally comprehensive, publicly available regional data

Major data transparency and measurement gap

State-Centered and Security-Driven Approach

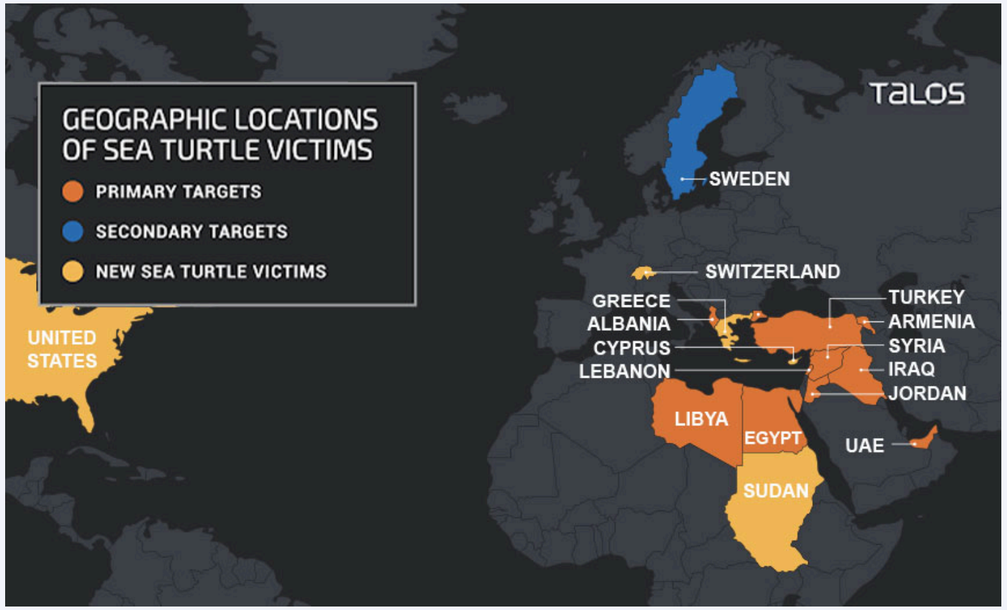
Cybercrimes Law, Telecom Regulation

Uneven Maturity and Limited Cooperation

Gulf States vs Levant

Politically Motivated

European Commission. (2022, February 1). Results of study on Domain Name System (DNS) Abuse. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/library/results-study-domain-name-system-dns-abuse



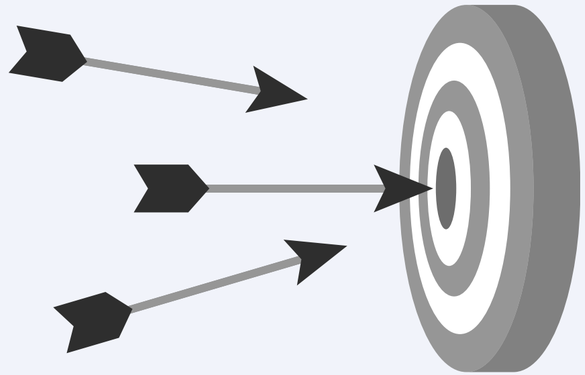
Example: Sea Turtle Campaign

Likely Threats

Threat	Likelihood	Primary Targets
DDoS campaigns against government portals	Very High	Israel, Gulf states, Jordan, US
Spear phishing and credential harvesting	Very High	NGOs, diplomats, defense contractors, media
ICS/OT targeting of energy infrastructure	High	Energy sector across the Middle East and Gulf
Hack-and-leak / doxxing operations	High	US military-linked entities, Israeli firms
Ransomware with political framing	High	Israeli and Gulf commercial targets
Wiper malware deployment	Moderate-High	High-value government and defense networks
Influence operations and fabricated breach claims	Very High	All sectors, designed to force public response

RH-ISAC, **The Middle East Conflict: Navigating the Geopolitical Landscape of Cyber Threats,** 2023.
https://rhisac.org/threat-intelligence/middle-east-conflict/

What is currently being done to tackle DNS abuse



01

Contractual Obligations

02

Industry Collaborations and Infrastructure Resilience

03

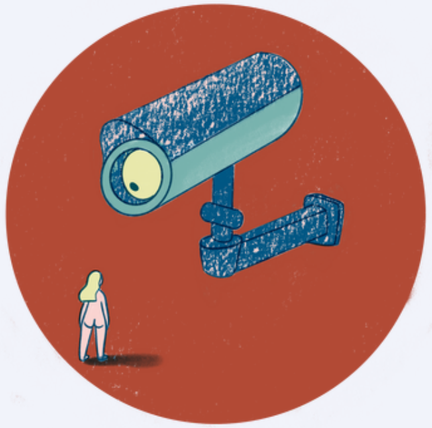
Policy Development

04

Suspension

ICANN85 Read Out on DNS Abuse Mitigation

Esho, G. (2026, April 3). My ICANN85 read out on DNS Abuse Mitigation. Medium. https://gbemiesho.medium.com/my-icann85-read-outon-dns-abuse-mitigation-2f5d78f99001



Why is suspension problematic?

Because DNS abuse mitigation frameworks could have significant human rights implications

Freedom of expression

Privacy

Right to Equal Treatment

Mitigation mechanisms should be available equally across service regions.

Freedom of Assembly

Access to Remedy

Individuals affected by takedowns or suspensions must have access to dispute resolution mechanisms.

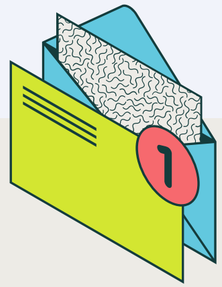
NO ONE-SIZE-FITS-ALL MODEL

Suggestions

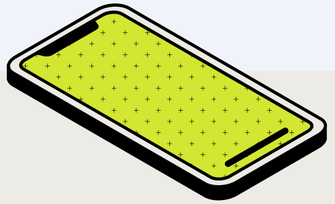
1	Reinforce the multi-stakholder model
2	Human Rights Impact Assessment (in lign with the recommendation from Article 19)
3	Principle of Proportionality + Develop safeguards against overblocking
4	Ensure clearer notice and appeal mechanisms
5	Strengthen transparency reporting
6	Conduct region specific studies

Thank you!

Open for questions



badranrym@gmail.com



LinkedIn
@rymbadran