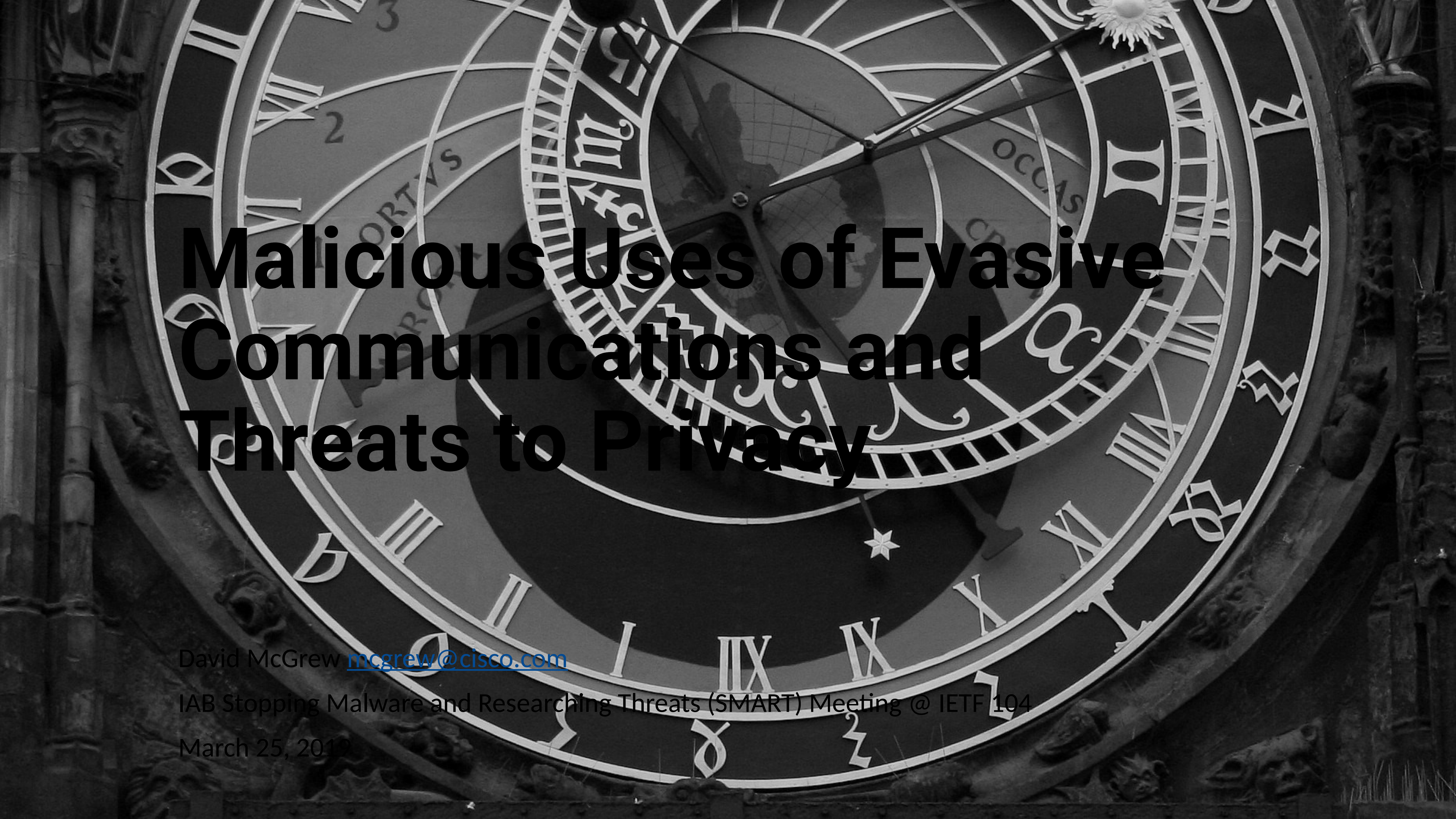


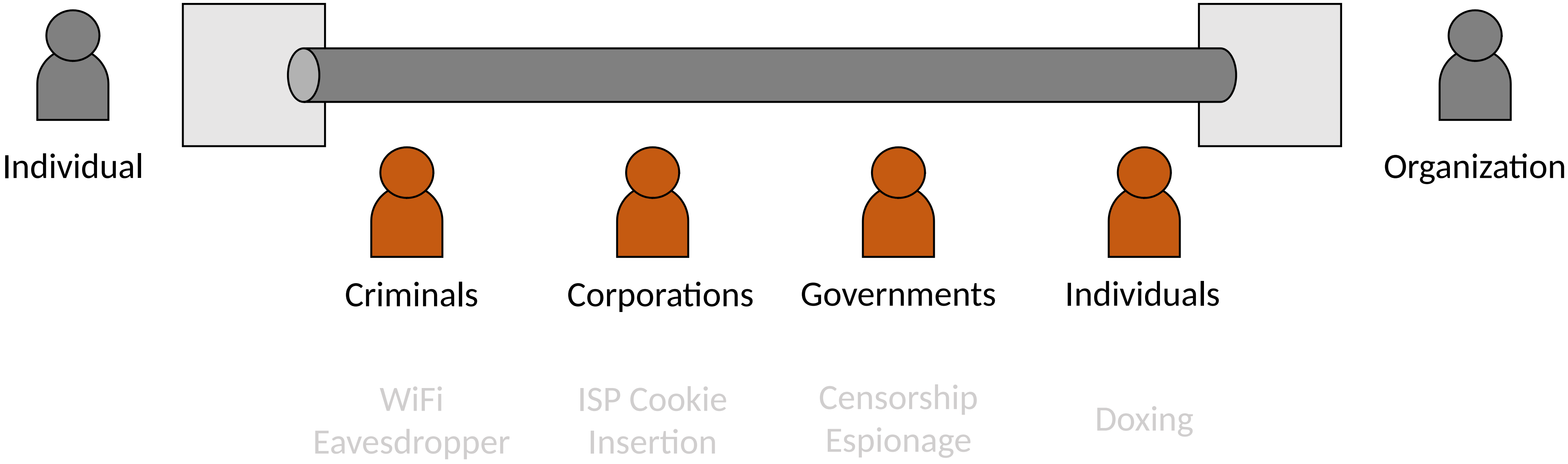
Malicious Uses of Evasive Communications and Threats to Privacy

David McGrew mcgrew@cisco.com

IAB Stopping Malware and Researching Threats (SMART) Meeting @ IETF 104

March 25, 2019

Privacy is a human right, and encrypted communication is a cornerstone of modern society



Evasive communication goals and uses

Goal	Benign Use	Malicious Use
Data confidentiality	Data privacy	Hide from defender
Evade blocking	Censorship circumvention	Infection, C2, exfiltration
Visit targeted site(s) without detection	Privacy	Minimize indications of compromise
Communication without detection	Hide circumvention	Hide infection

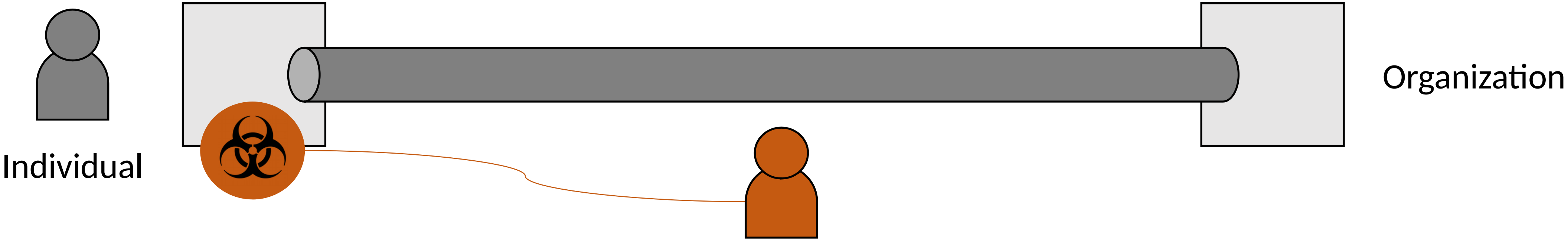
Goals are applicable to DoH, DoT, eSNI, Domain Fronting, and other protocols

Evasive communication goals and uses

Goal	Benign Use	Malicious Use
Data confidentiality	Data privacy	Hide from defender
Evade blocking	Censorship circumvention	Infection, C2, exfiltration
Visit targeted site(s) without detection	Privacy	Minimize indications of compromise
Communication without detection	Hide circumvention	Hide infection

Goals are applicable to DoH, DoT, eSNI, Domain Fronting, and other protocols

Client-side attacks on privacy



"Remote Administration Tools (RAT) provide the ability to remotely survey the electronic activities of a victim by keylogging, remote desktop viewing, webcam spying, audio-eavesdropping, data exfiltration, and more."

Syrian Activists Targeted with BlackShades Spy Software (Citizen Lab, 2012)

Client-side attacks against privacy: examples

- Over the last decade, Syrian activists have been targeted by malware including DarkComet, Blackshades, Xtreme RAT Trojan, njRAT, ShadowtechRAT, Dark Caracal, and infected Freegate clients
- Similar tactics against activists, lawyers, and journalists in Mexico, Azerbaijan, Egypt, and United Arab Emirates have been documented
- In many cases, the victims were tricked into installing malware, including infected evasive communications applications

> *"... all Dark Caracal needed was application permissions that users themselves granted when they downloaded the apps, not realizing that they contained malware," said EFF Staff Technologist Cooper Quintin. "This research shows it's not difficult to create a strategy allowing people and governments to spy on targets around the world."*

EFF and Lookout Uncover New Malware Espionage Campaign Infecting Thousands Around the World; Mobile Devices Compromised by Fake Secure Messaging Clients – Hundreds of Gigabytes of Data Stolen (EFF)

Client-side attacks against privacy: examples

Campaign Targeting Syrian Activists Escalates with New Surveillance Malware (EFF)

HOW THE BOY NEXT DOOR ACCIDENTALLY BUILT A SYRIAN SPY TOOL (WIRED)

Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns (Citizen Lab and EFF)

A CALL TO HARM - New Malware Attacks Target the Syrian Opposition (Citizen Lab)

When Governments Attack: Malware Targeting Activists, Lawyers, and Journalists (Eva Galperin, EFF)

Commercial spyware unleashed against Mexican Political Activists (SOPHOS, 2017)

False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan (Amnesty International, 2017)

PROMINENT HUMAN RIGHTS ACTIVISTS IN EGYPT TARGETED BY SOPHISTICATED HACKING ATTACKS (The Intercept, 2017)

Egyptian activists and media targeted by phishing attacks (Reuters, 2019)

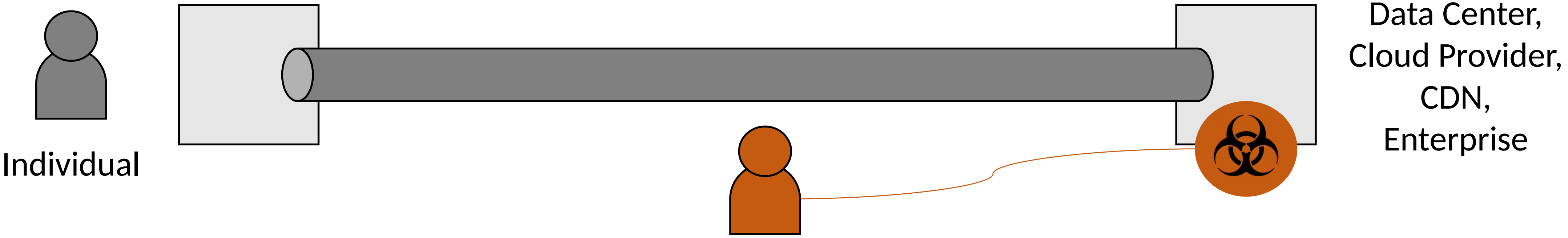
The UAE Spends Big on Israeli Spyware to Listen In on a Dissident (Foreign Policy, 2016)

Syrian Activists Targeted with BlackShades Spy Software (Citizen Lab, 2012)

EFF and Lookout Uncover New Malware Espionage Campaign Infecting Thousands Around the World (EFF)

How the FBI found Miss Teen USA’s webcam spy (Ars Technica, 2013)

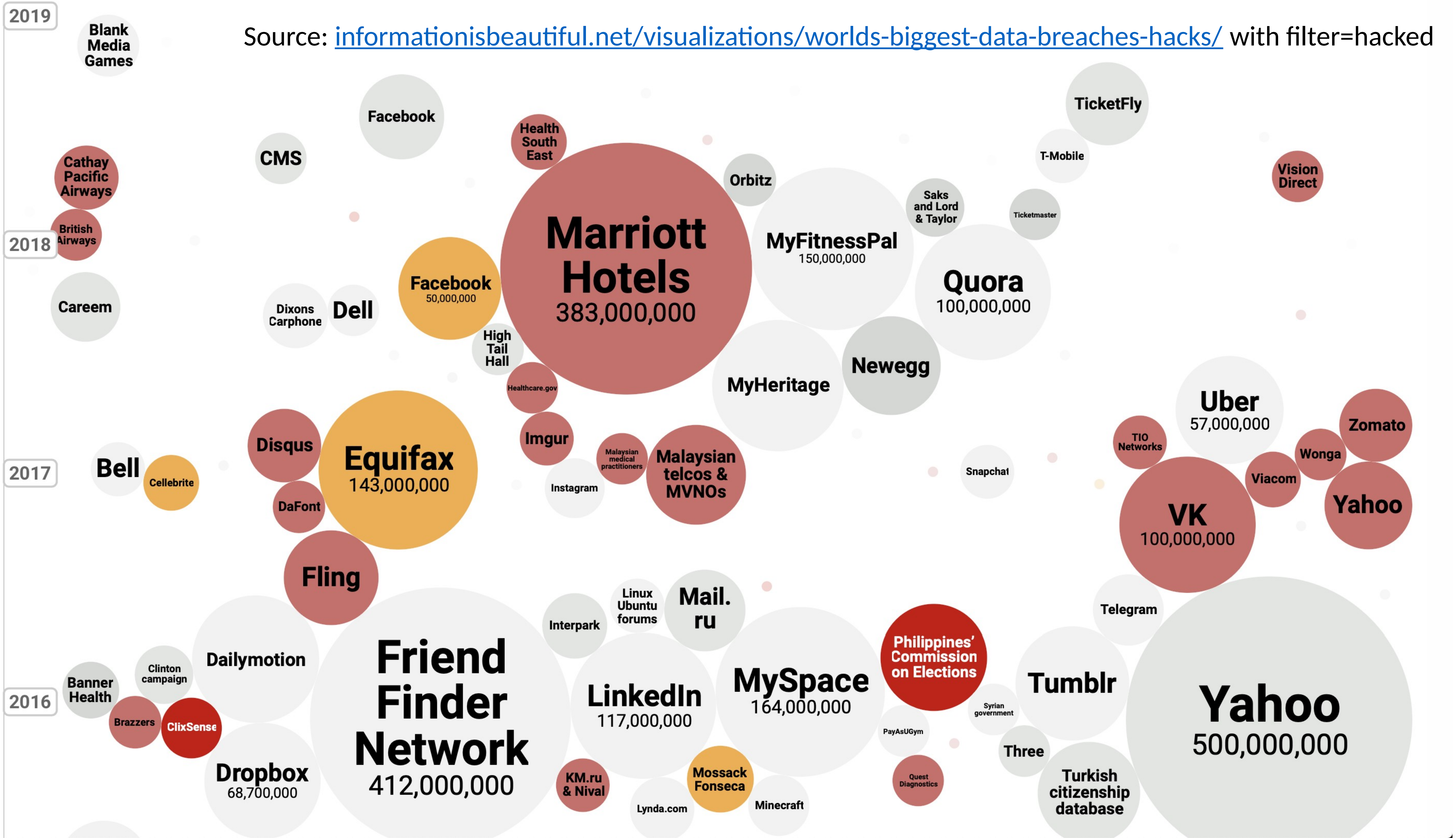
Server-side attacks on privacy



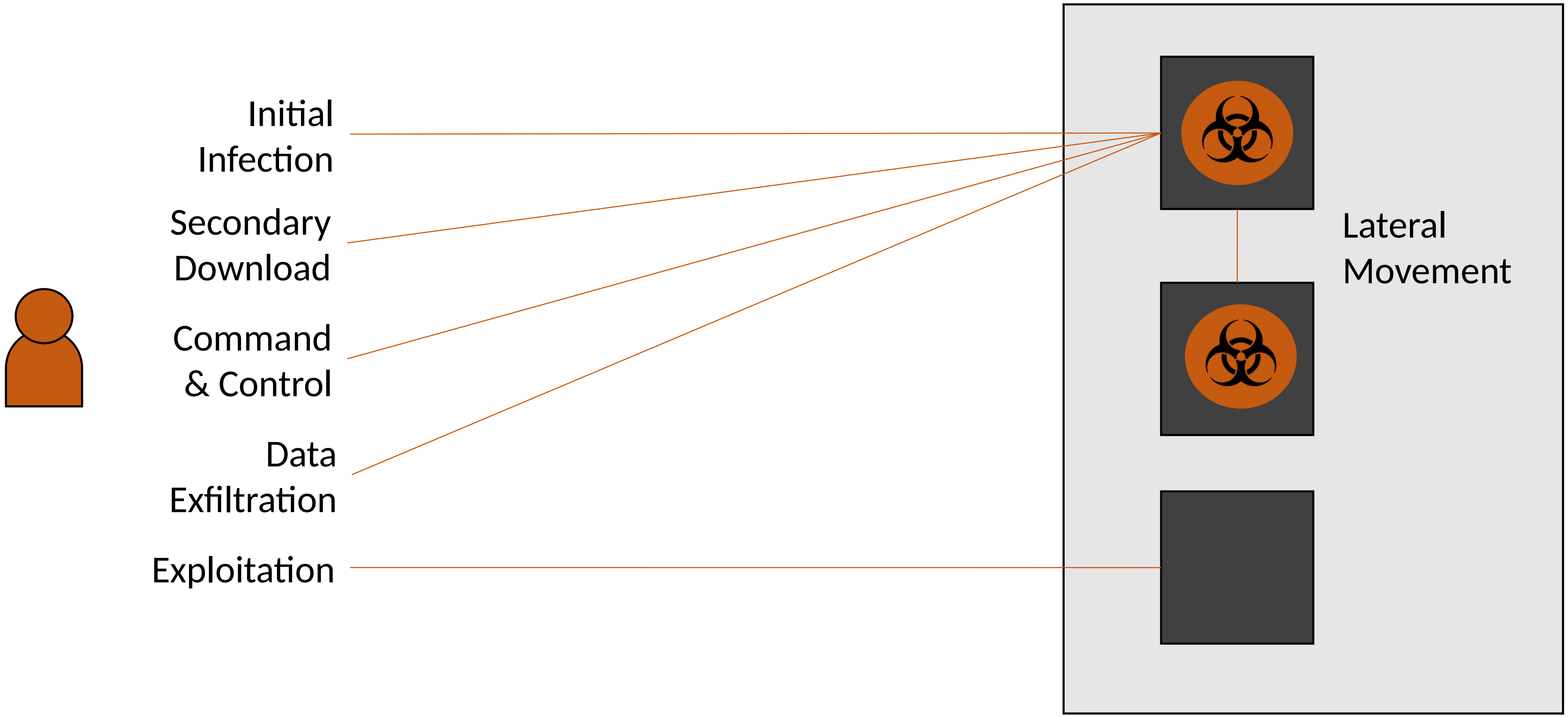
"[With] any large network, I will tell you that persistence and focus will get you in, will achieve that exploitation without the zero days … There's so many more vectors that are easier, less risky and quite often more productive than going down that route."

Rob Joyce, NSA TAO, in *NSA HACKER CHIEF EXPLAINS HOW TO KEEP HIM OUT OF YOUR SYSTEM* (WIRED, 2016)

Source: informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ with filter=hacked



Server-side attacks on privacy



Stolen Passwords

… The monster data dump goes by the prosaic "Collection #1" and contains 1.16B unique combinations of email addresses and passwords, but only 772 million unique email addresses. It's the largest data dump to ever be loaded into Have I Been Pwned, and it represents a sort of meta-breach collection rather than the results of any single security exploit or corporate security shortfall.

New Massive Security Breach Exposes 773 Million Passwords
(ExtremeTech, 2019)

Malware’s use of evasive communication

Observed in malware sandbox with strong convictions (> 5 AV signatures excluding adware)

TLS sessions	1,894,926
Nonstandard ports	2.37%
Tor	3.42%
Ultrasurf	0.214%
Psiphon	0.0261%
Torch	0.0541%
Citrio	0.0867%
1stbroswer	0.00100%

Source: Blake Anderson

Malware’s use of evasive communication

Observed in malware sandbox with strong convictions (> 5 AV signatures excluding adware)

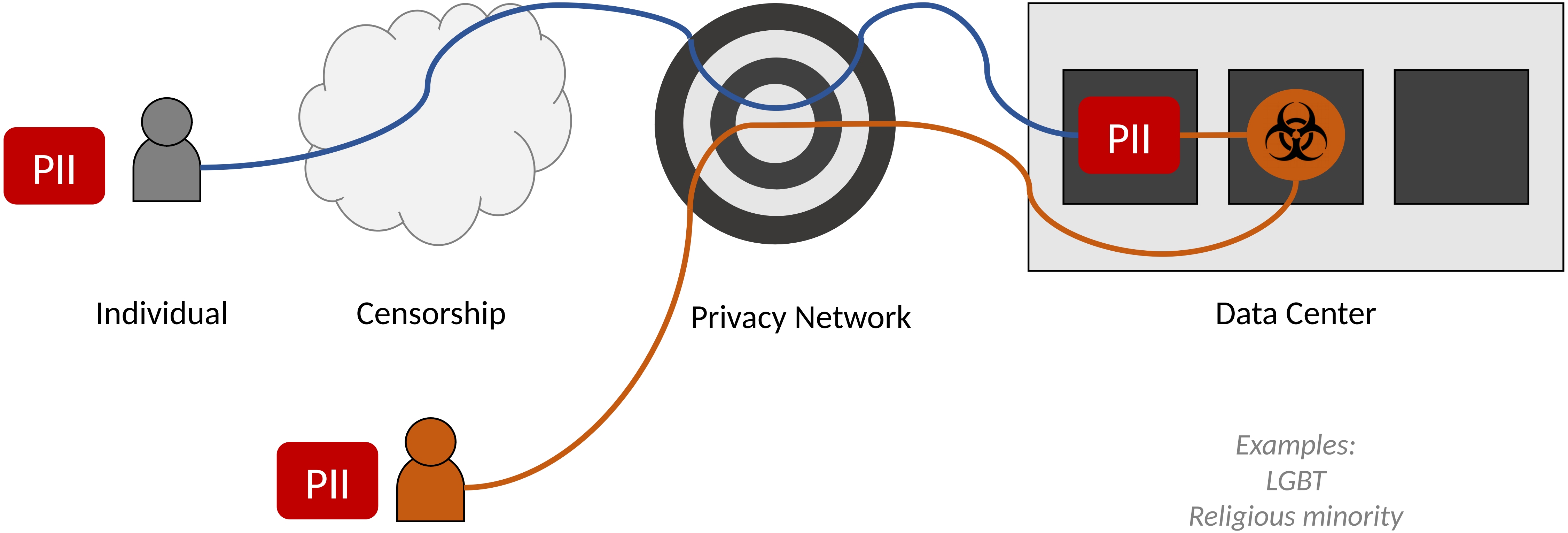
TLS sessions	1,894,926
Nonstandard ports	2.37%
Tor	3.42%
Ultrasurf	0.214%
Psiphon	0.0261%
Torch	0.0541%
Citrio	0.0867%
1stbroswer	0.00100%

Secondary downloads and C2

dropbox.com. dropboxusercontent.com. onedrive.com, drive.google.com, docs.google.com, googleusercontent.com, githubusercontent.com, github.com

Source: Blake Anderson

Evasion blowback against privacy



Examples:
LGBT
Religious minority
Democracy advocate
Journalist

Research Questions

- Can malware's use of evasive technology be further characterized?
- Can evasive technologies prevent malware from utilizing their services without reducing privacy for other users?
- Can an evasive client or OS provide a strong assurance of the absence of malicious/unauthorized communication to its user or admin?
- How can protocol designers prevent or mitigate malicious uses?

Conclusions

- We need to defend against *all* threats to privacy and security
- Evasive communication techniques are used by malicious actors
- Open research questions

THANKS