Inside the FBI's Secret Encrypted Phone Company 'Anom'

Joseph Cox // DEF CON 32

Location: SA



Domenico CATANZARITI

- CATANZARITI: A mate of mine has imported a welder with his mates company... UPS has ramg up and said they need a broker to sign the paper work off for customs, is that something u can do



- CATANZARITI: A mate of mine has imported a welder with his mates company... UPS has ramg up and said they need a broker to sign the paper work off for customs, is that something u can do

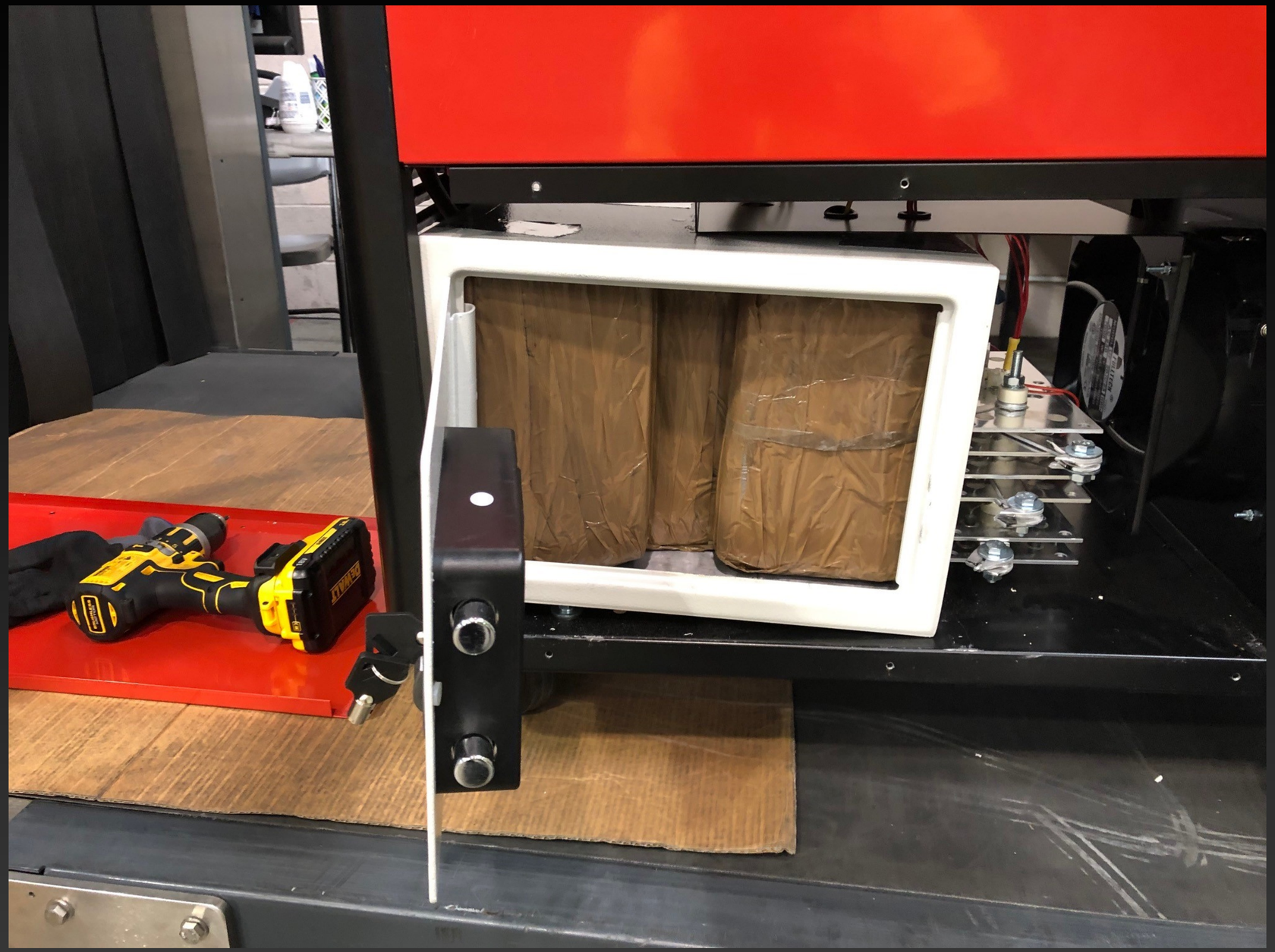
- CATANZARITI: Lol. U kill me. Pieces. Bricks. Keys. Keys. Rack. Robba. Coca. Ok lets make millions





Something’s wrong…

“Pigs grabbed him”


DEWALT

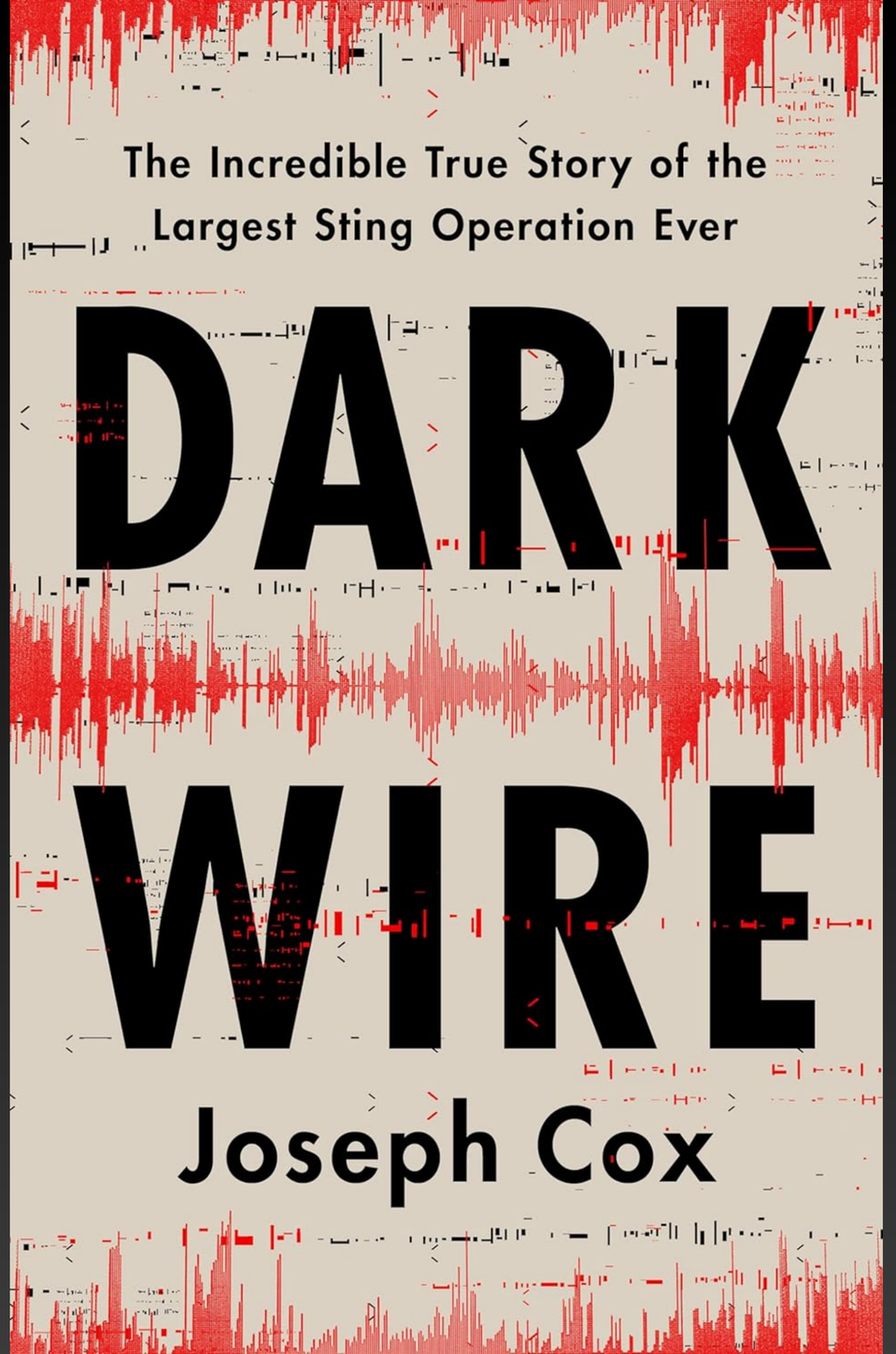

FEDERAL BUREAU OF INVESTIGATION

Who Is This Guy?

Joseph Cox

- Author of DARK WIRE
- Co-founder of 404 Media
- Former Motherboard journalist

404 MEDIA



Who Is This Guy?
Joseph Cox

- Spoke to:
  - Phone coders
  - Phone sellers
  - Drug traffickers
  - FBI agents
  - Other law enforcement officials
  - Got lots, LOTS of docs...





Inside the FBI’s Secret Encrypted Phone Company ‘Anom’

Agenda

Inside the FBI’s Secret Encrypted Phone Company ‘Anom’
Agenda

- The Phone
  - Software, hardware, network, FBI front-end interface

Inside the FBI's Secret Encrypted Phone Company 'Anom'

Agenda

- The Phone
  - Software, hardware, network, FBI front-end interface
- The Structure of Anom
  - The coders, sellers, users, and FBI

Inside the FBI's Secret Encrypted Phone Company 'Anom'

Agenda

- The Phone
  - Software, hardware, network, FBI front-end interface
- The Structure of Anom
  - The coders, sellers, users, and FBI
- Microsoft and "Black Boxes"
  - Why Anom started to grow out of control

Inside the FBI's Secret Encrypted Phone Company 'Anom'
Agenda

- The Phone
  - Software, hardware, network, FBI front-end interface
- The Structure of Anom
  - The coders, sellers, users, and FBI
- Microsoft and "Black Boxes"
  - Why Anom started to grow out of control
- What This All Means for the Going Dark Debate
  - What was this operation's impact, and what happens now?

The Phone
(and the backdoor)



The Phone
Hardware





- Google Pixel 4a

The Phone

Hardware





- Google Pixel 4a
- Google Pixel 2
- Google Pixel 3a
- Samsung Galaxy A30S
- Samsung Galaxy S20
- Samsung Note 10+
- Xiaomi A2 Lite
- Xiaomi A3

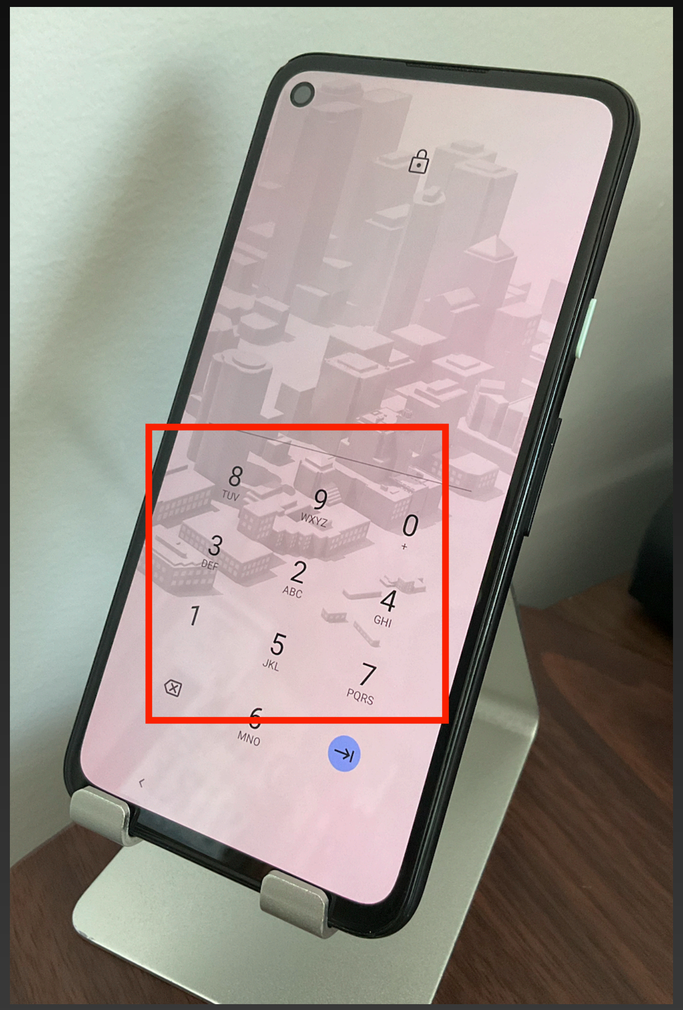
The Phone
Hardware

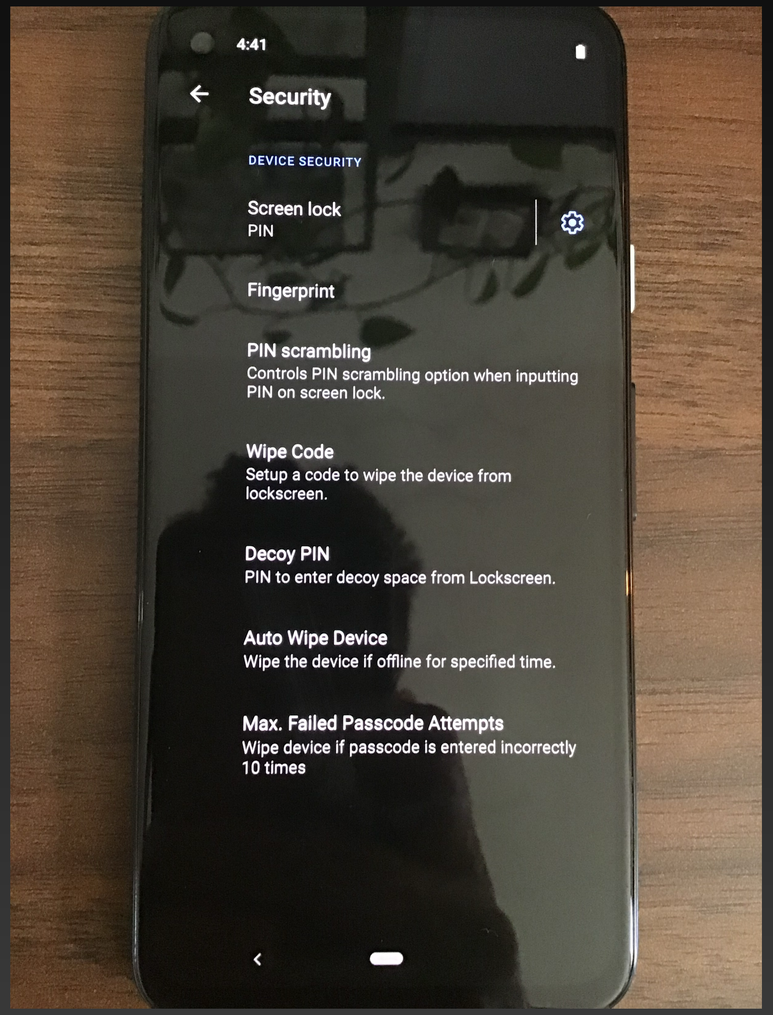


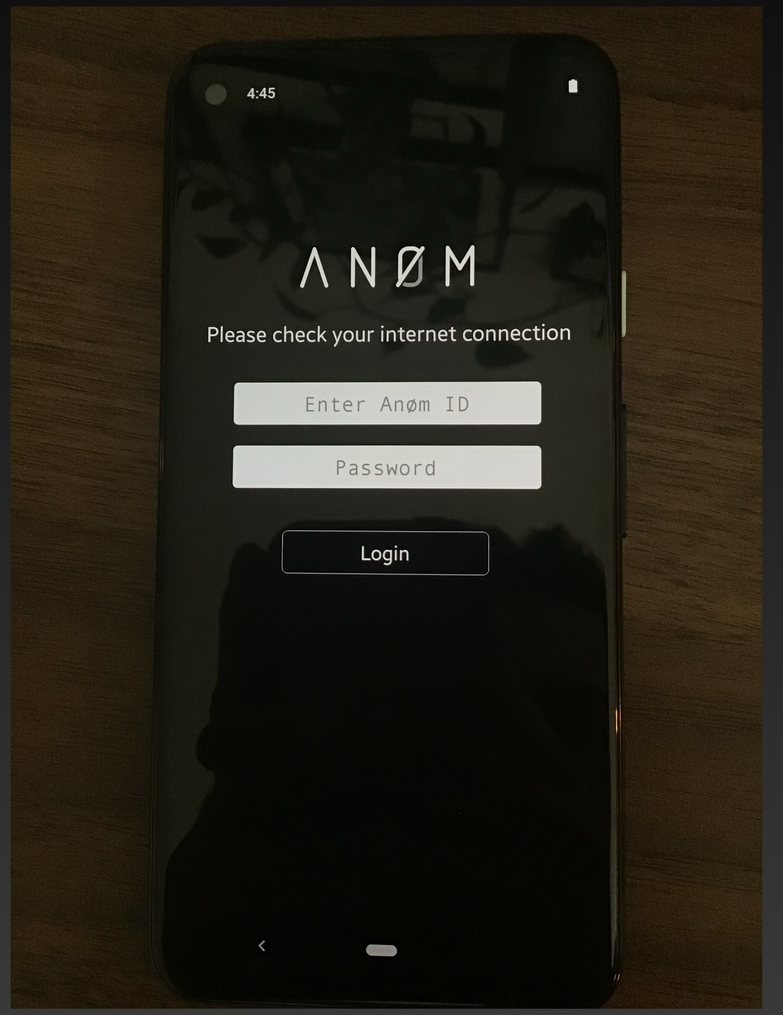
Image: Laserlicht via Wikipedia.

- Intel Next Unit of Computing (NUC)

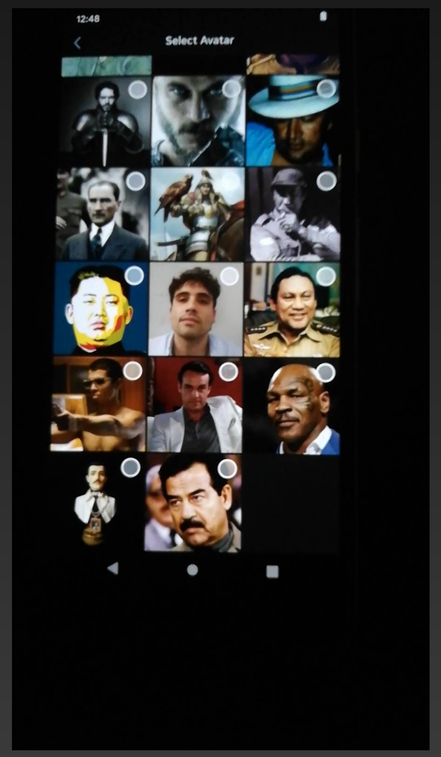
The Phone
Software

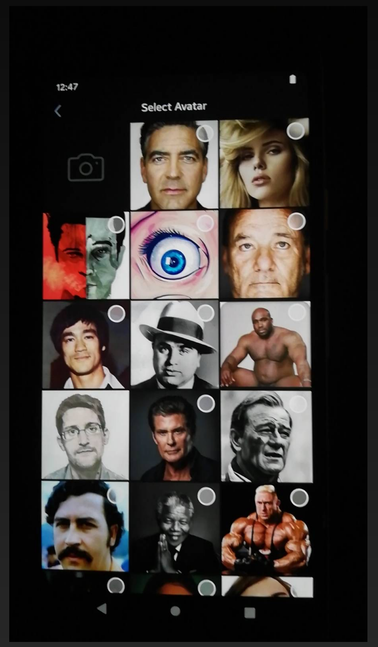


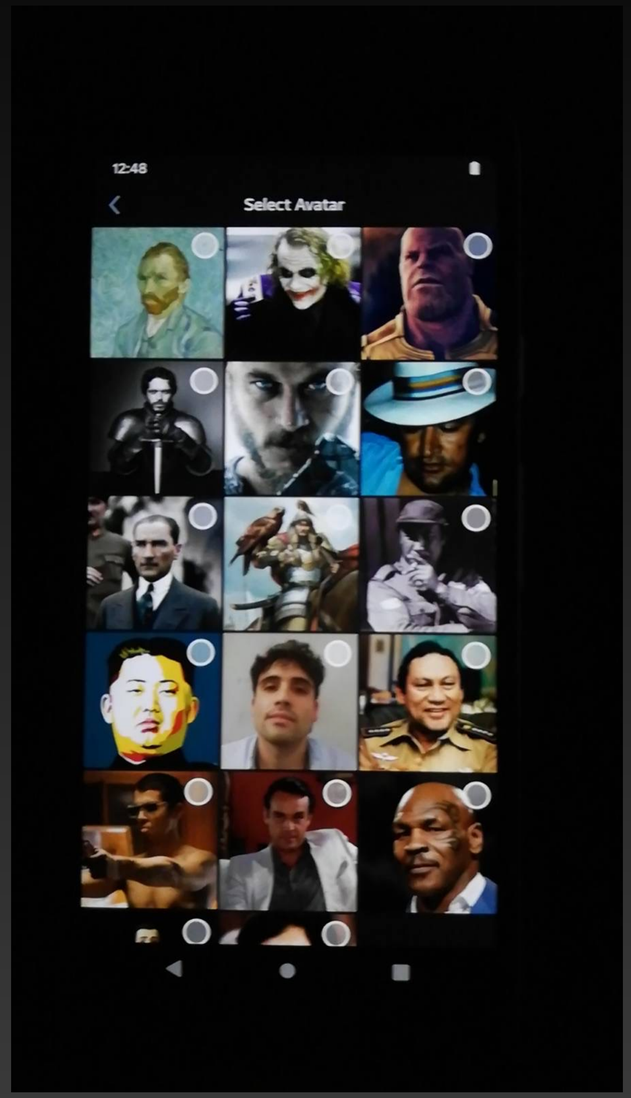


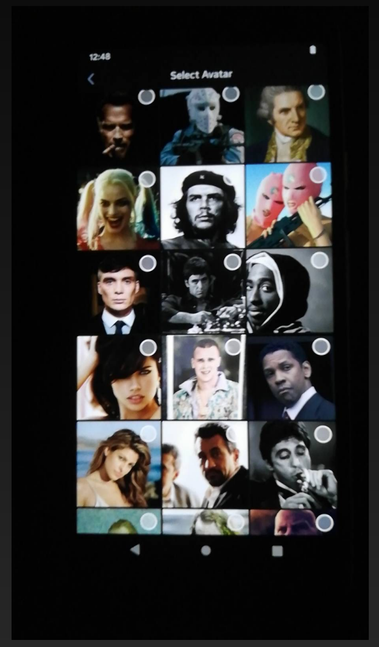


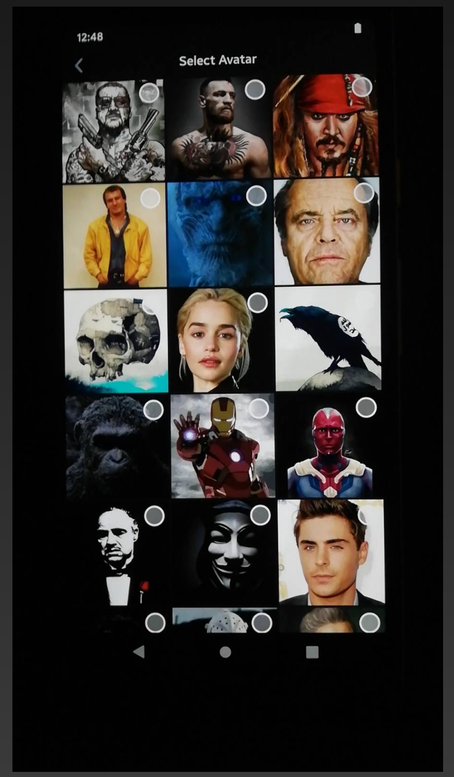
The Phone
The Software





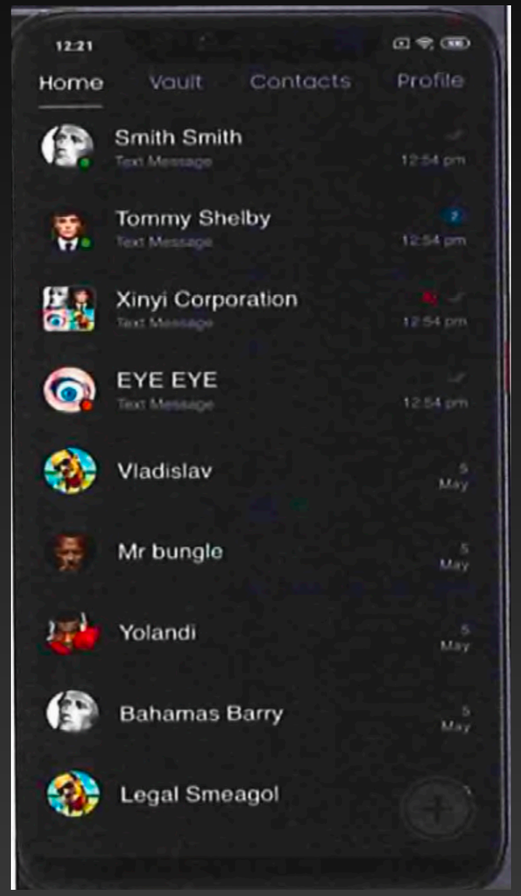






The Phone

The Software



The Phone

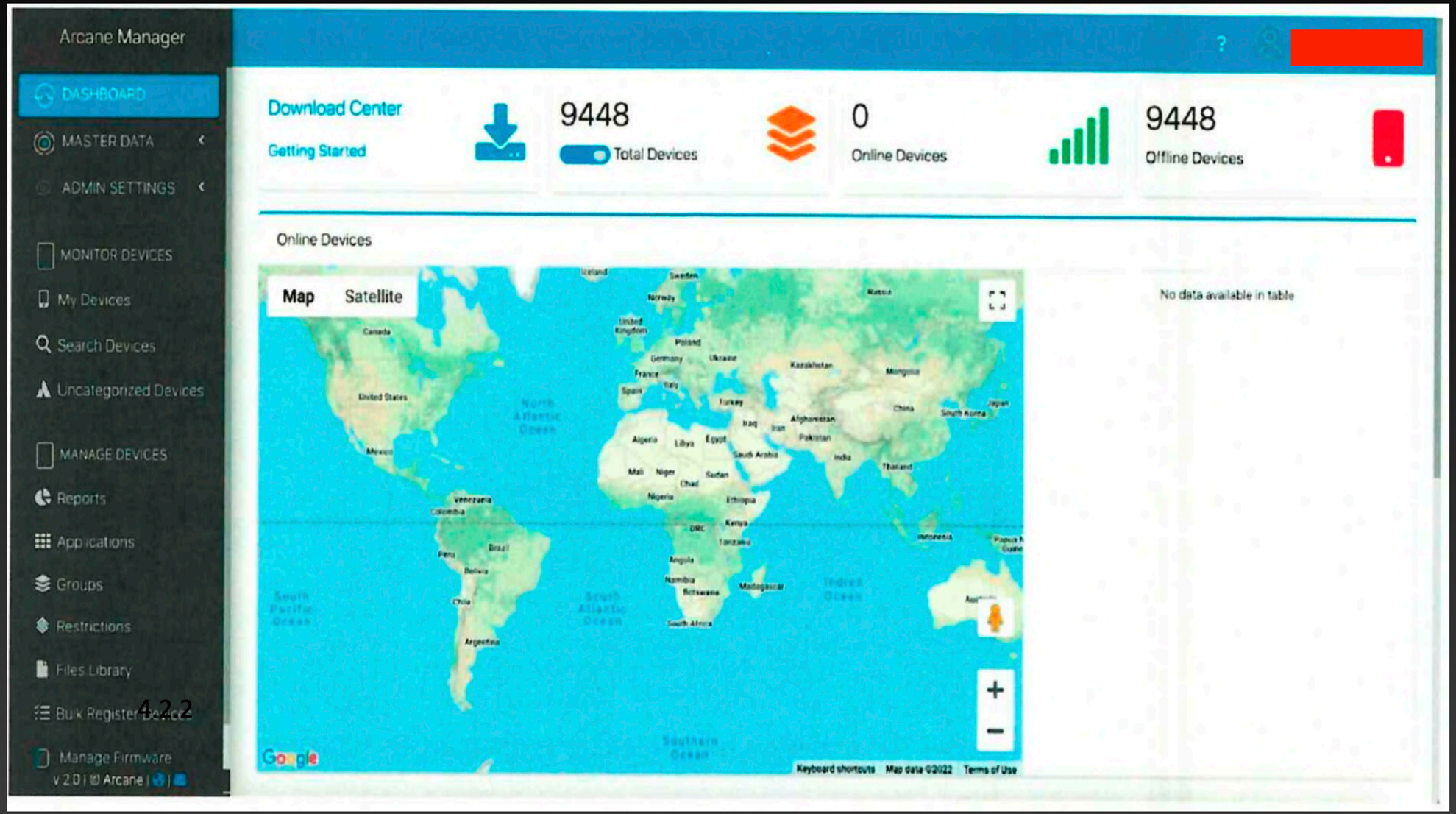
The MDM





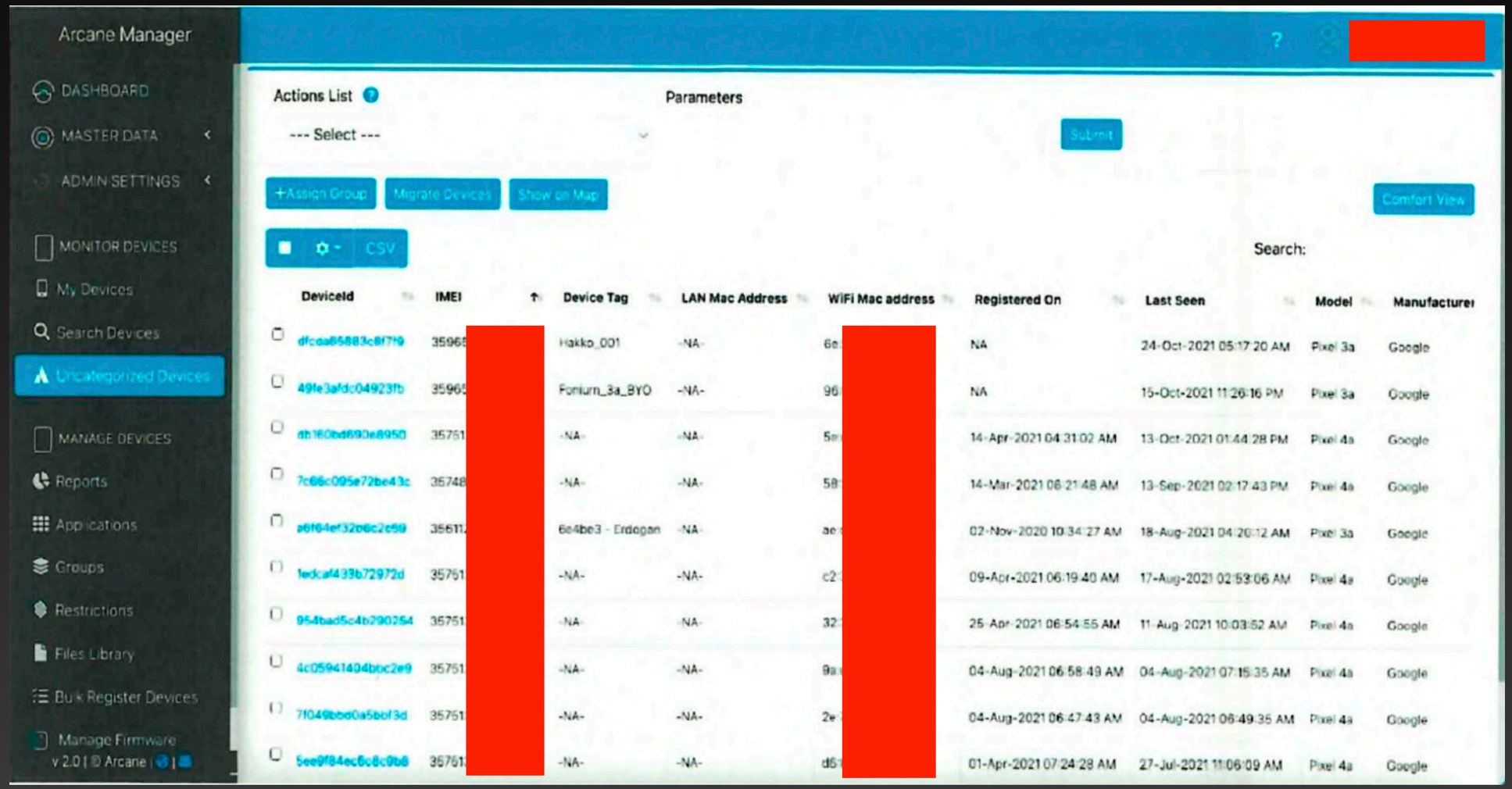
The Phone

Arcane Manager



422

The Phone
Arcane Manager

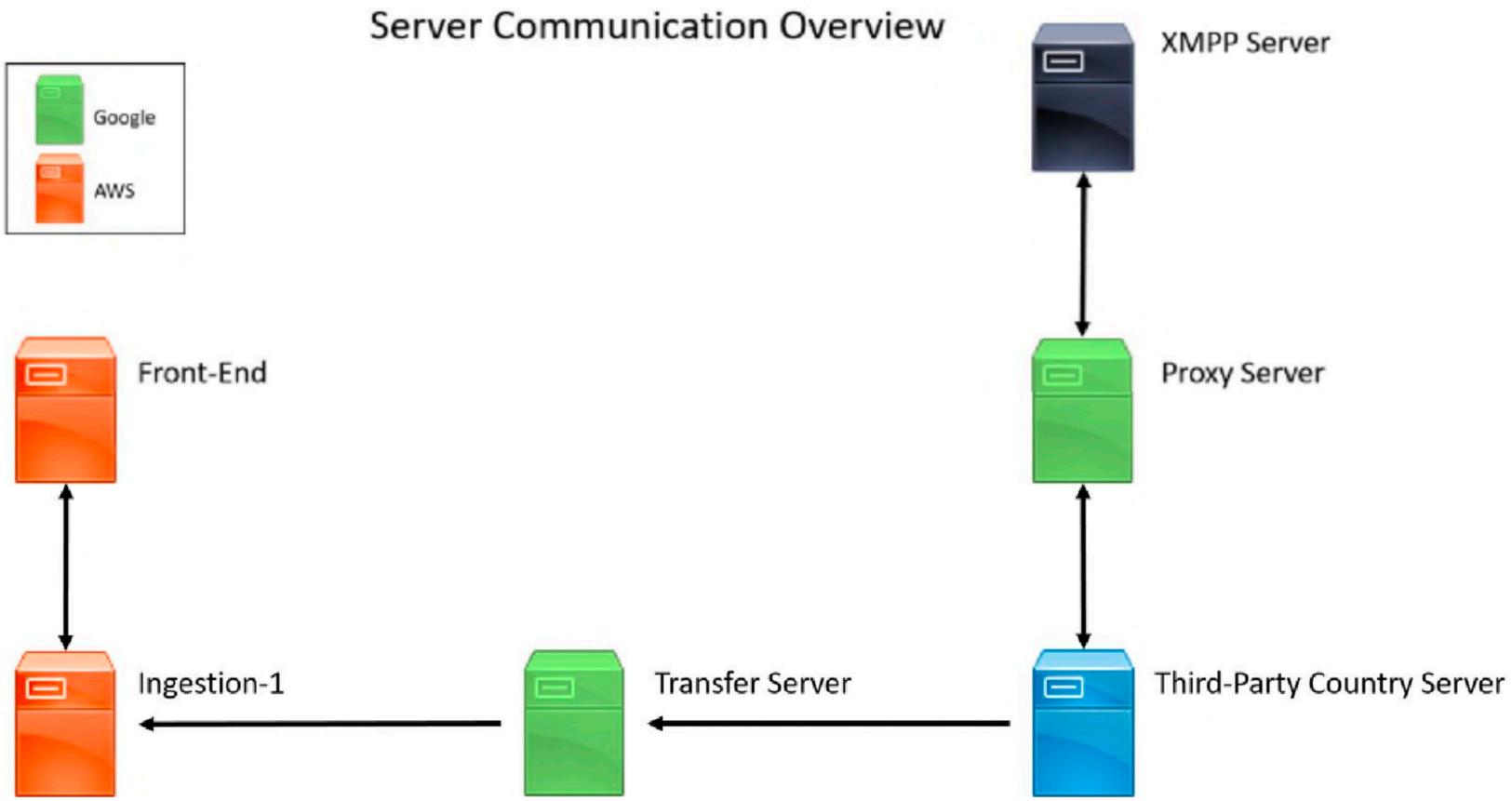


The Phone

Arcane Manager

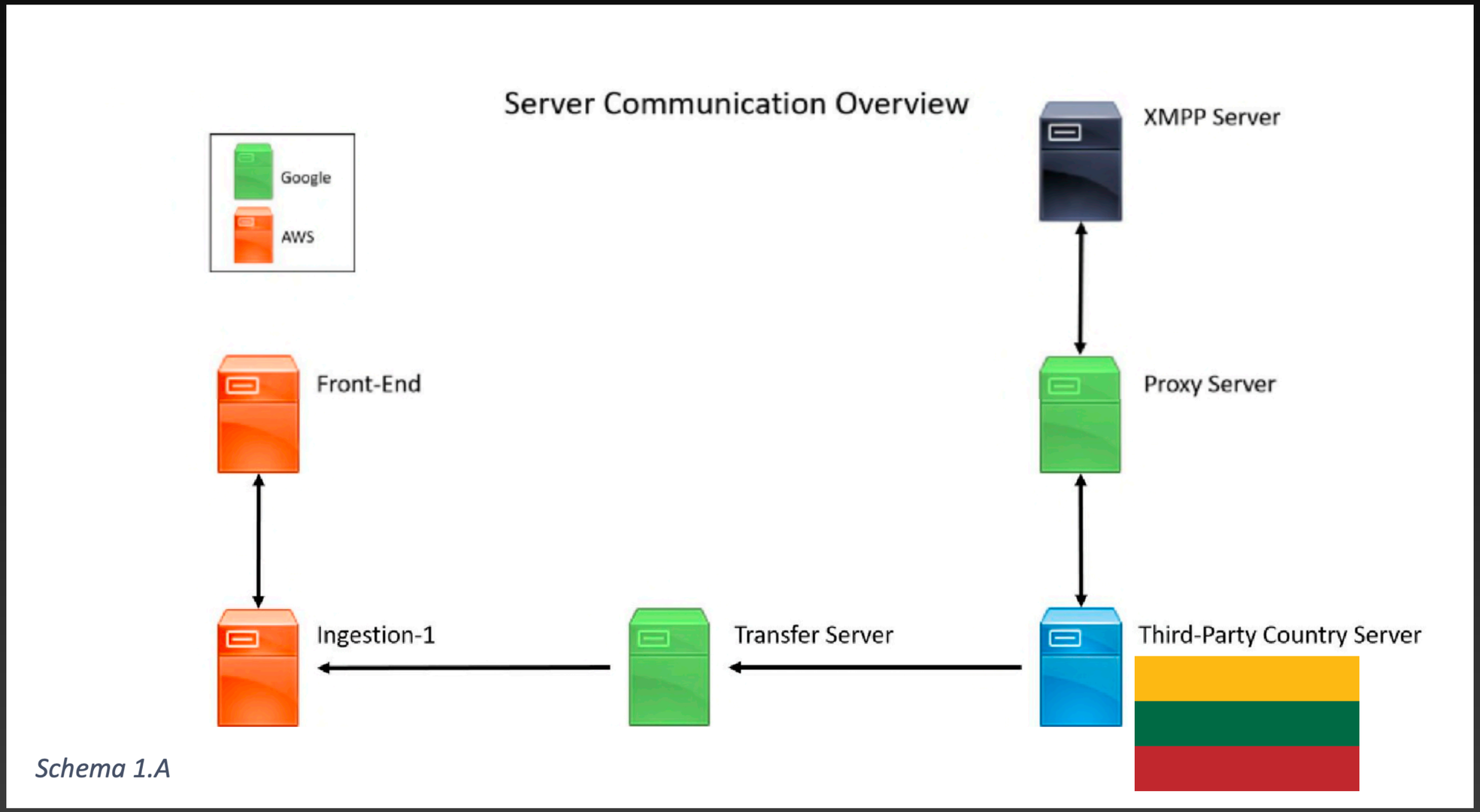


The Phone
The Infrastructure



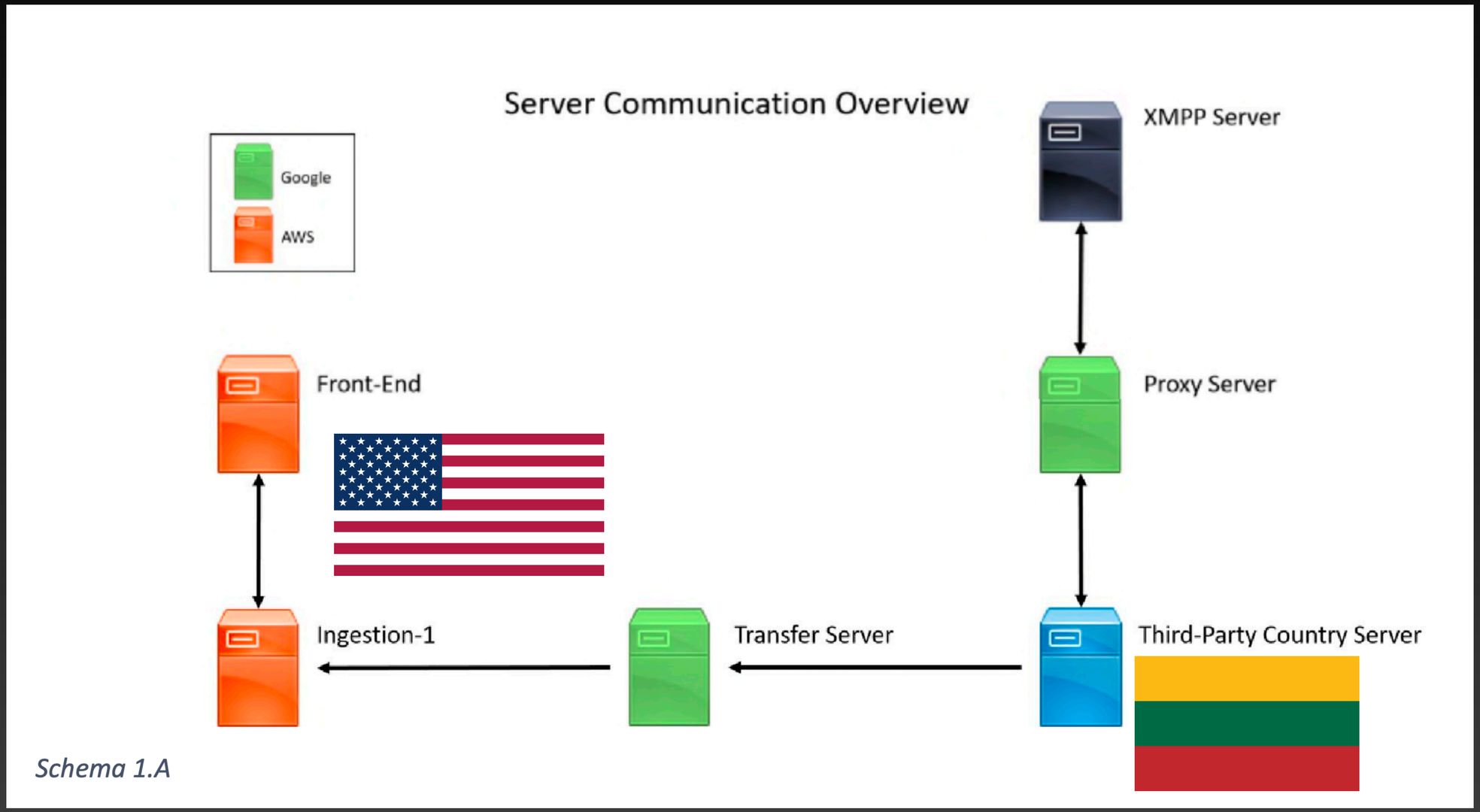
Schema 1.A

The Phone
The Infrastructure



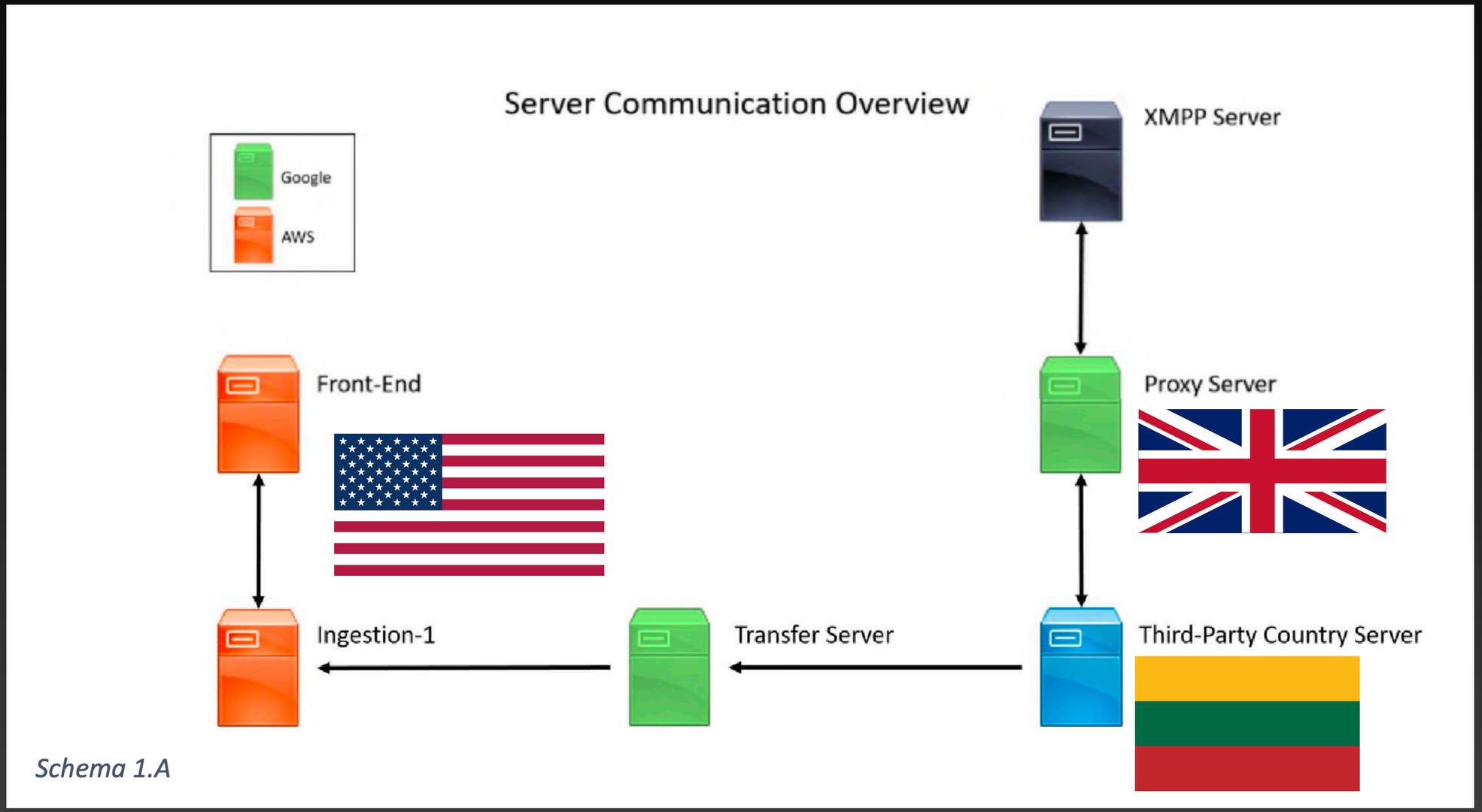
Schema 1.A

The Phone
The Infrastructure



Schema 1.A

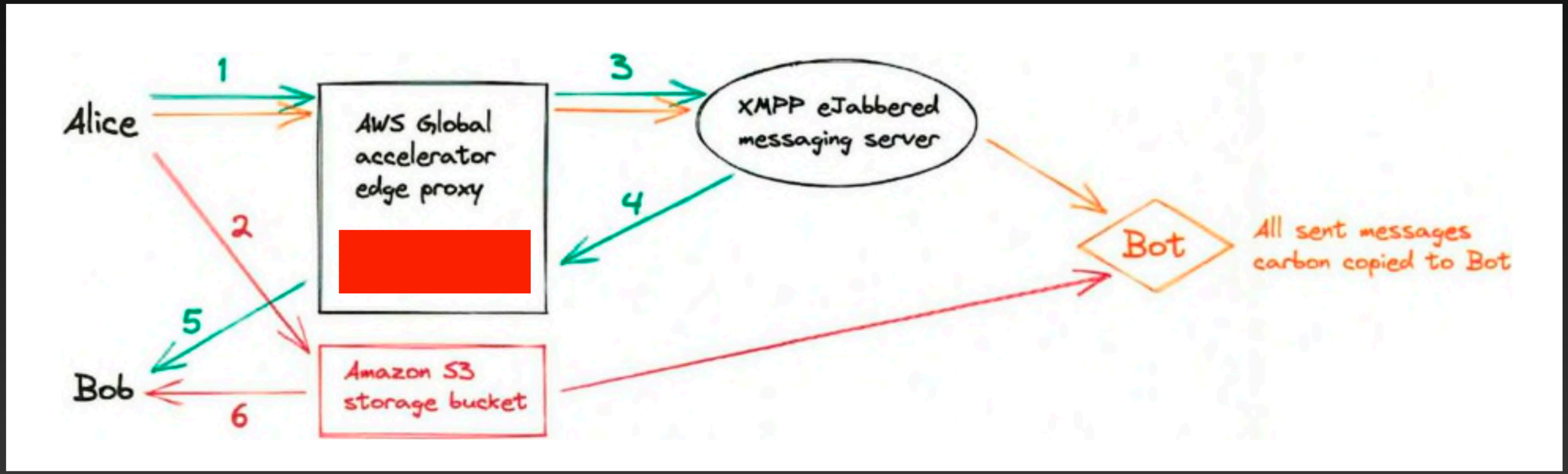
The Phone
The Infrastructure



Schema 1.A

The Phone

The Backdoor



The Phone

The Backdoor

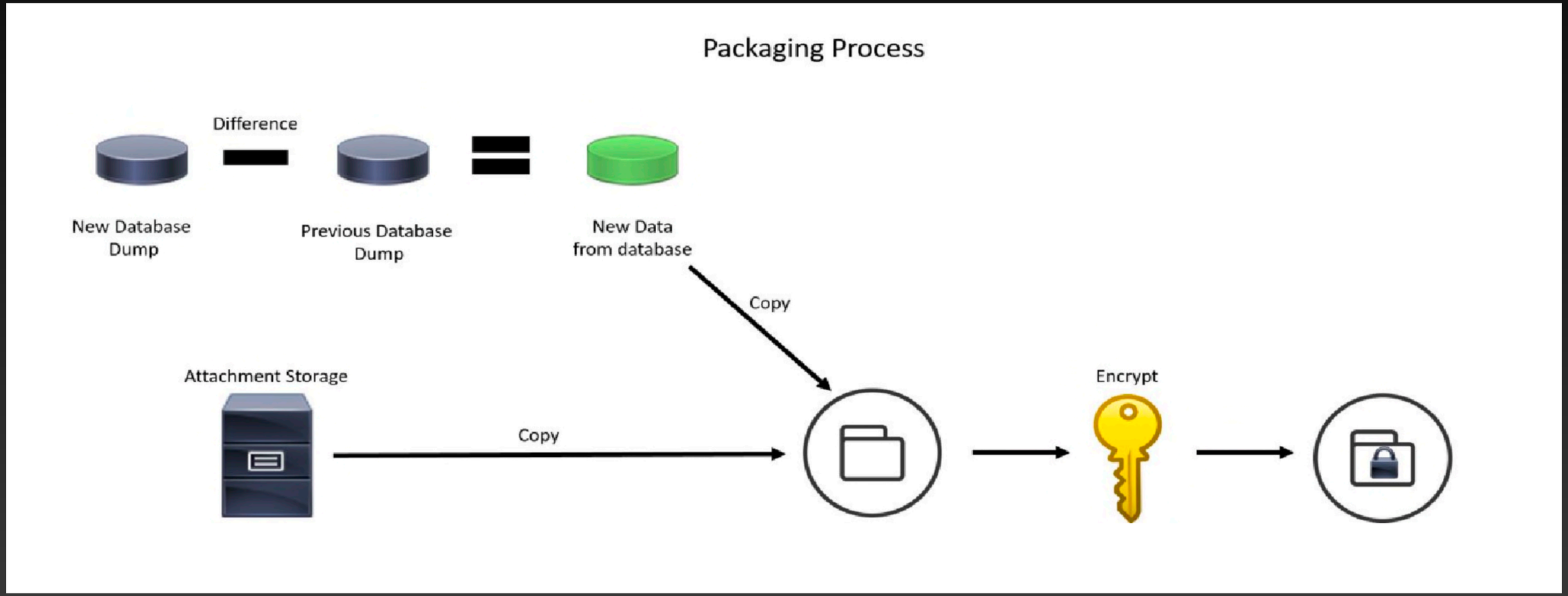
```
/* renamed from: k */
public final String f18651k = "echo@[redacted]

/* renamed from: l */
public final String f18652l = "support@[redacted]

/* renamed from: m */
public final String f18653m = "bot@[redacted]

/* renamed from: n */
public final String f18654n = "backup@[redacted]
```

The Phone

The Backdoor

```
this.f22974j.f20021K.mo28441a(c, z);
String aVar = eVar.mo28620P().mo32932q().toString();
AnomApplication.m30407i().getClass();
if (aVar.equalsIgnoreCase("bot@[redacted] = [redacted]()) != null) {
    [redacted]("Bot got recreated at the server", new Object[0]);
    C5296l lVar = new C5296l(f, "", f.mo29179i0());
    lVar.mo29229A1(6);
    this.f22974j.mo30424R3(lVar);
}
```

The Phone
The Backdoor



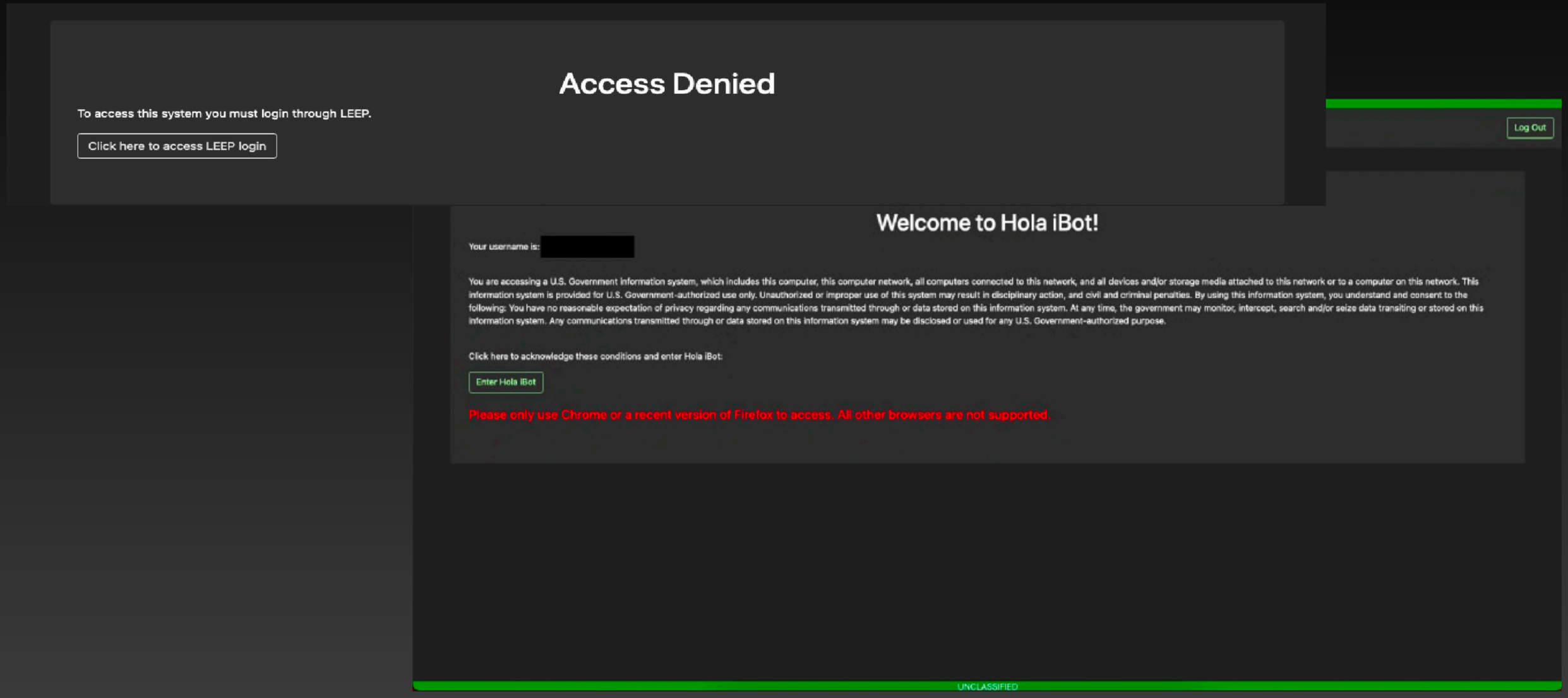
The Interface

HolaiBot



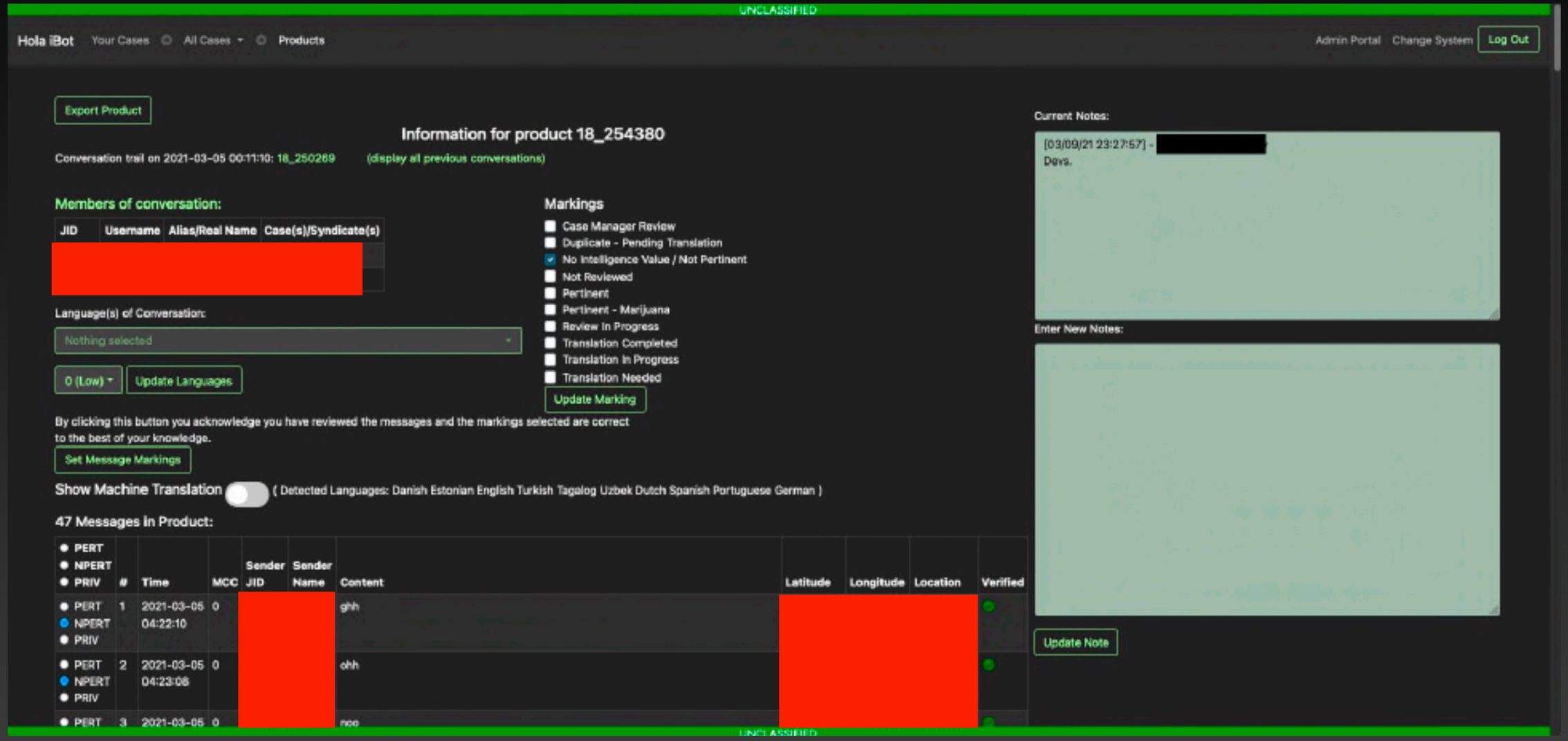
The Interface

HolaiBot



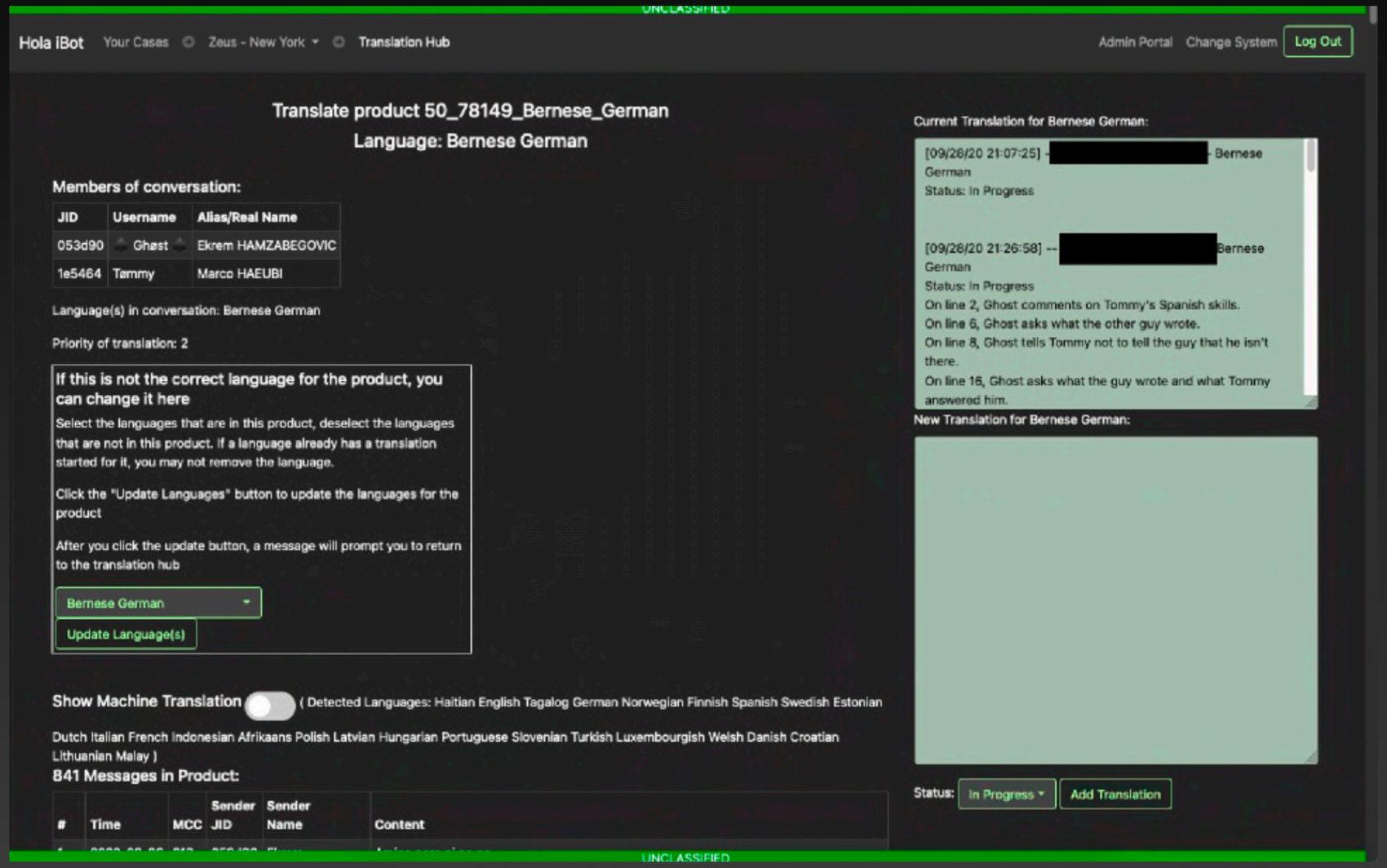
The Interface

HolaiBot



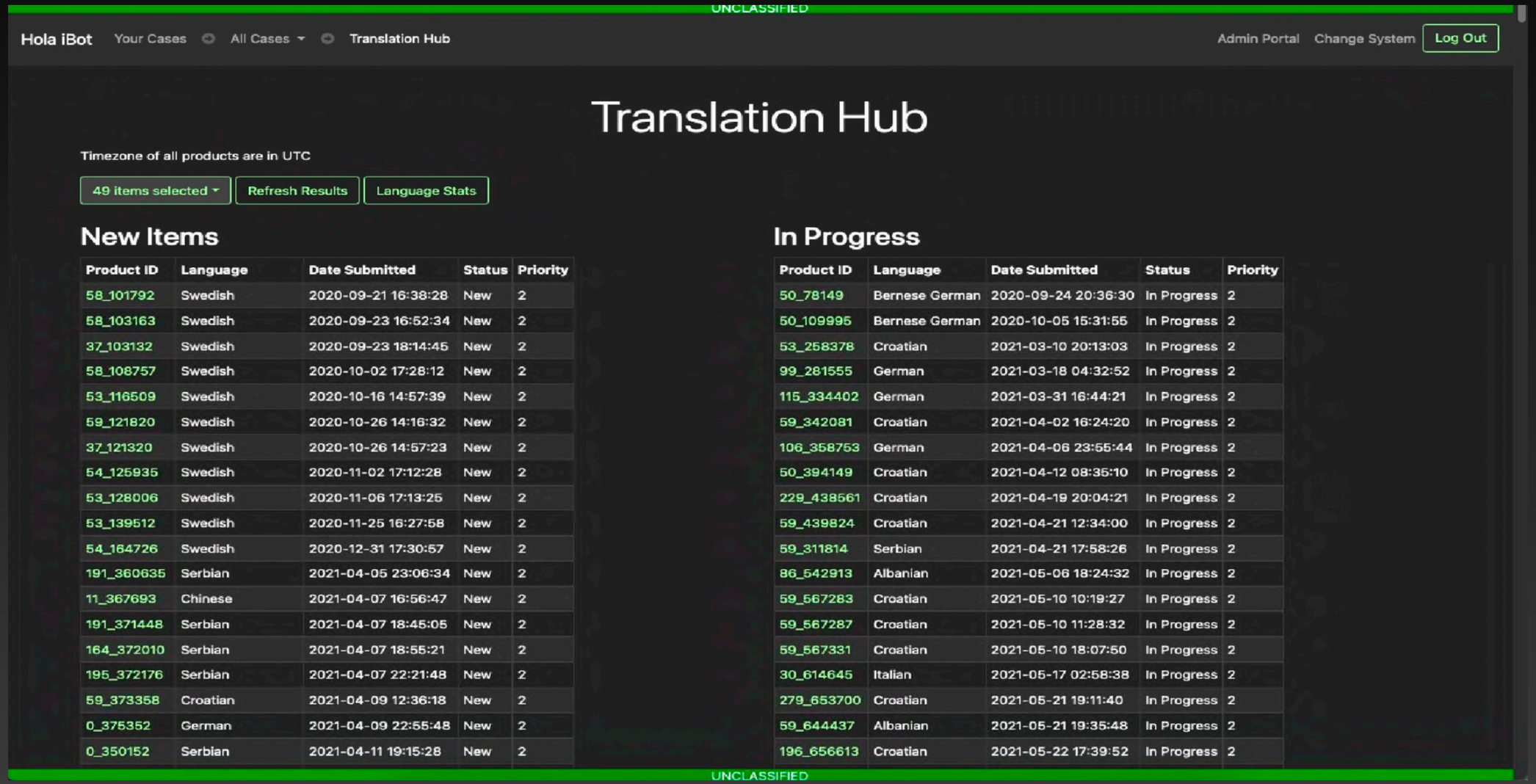
The Interface

HolaiBot



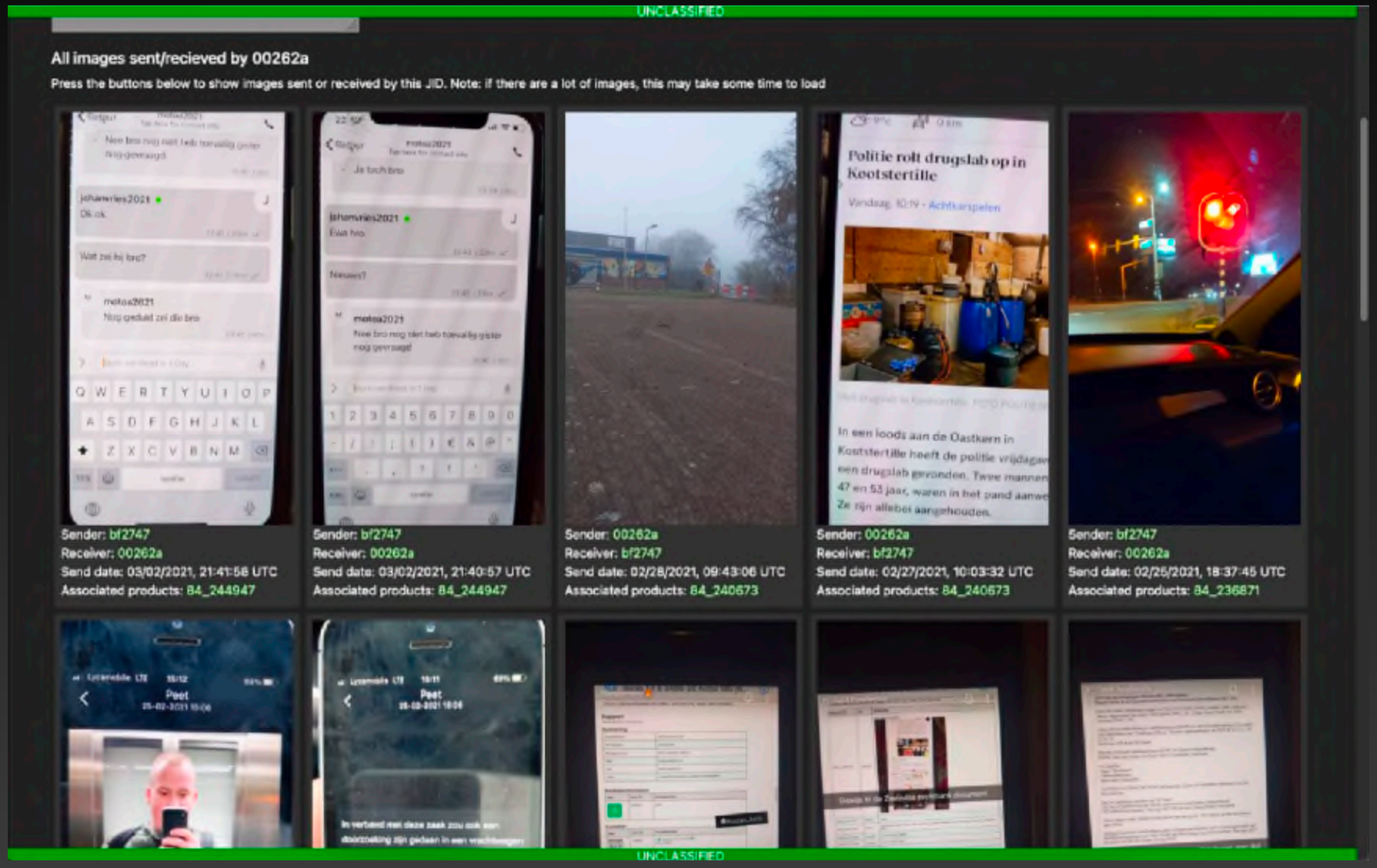
The Interface

HolaiBot



The Interface

HolaiBot



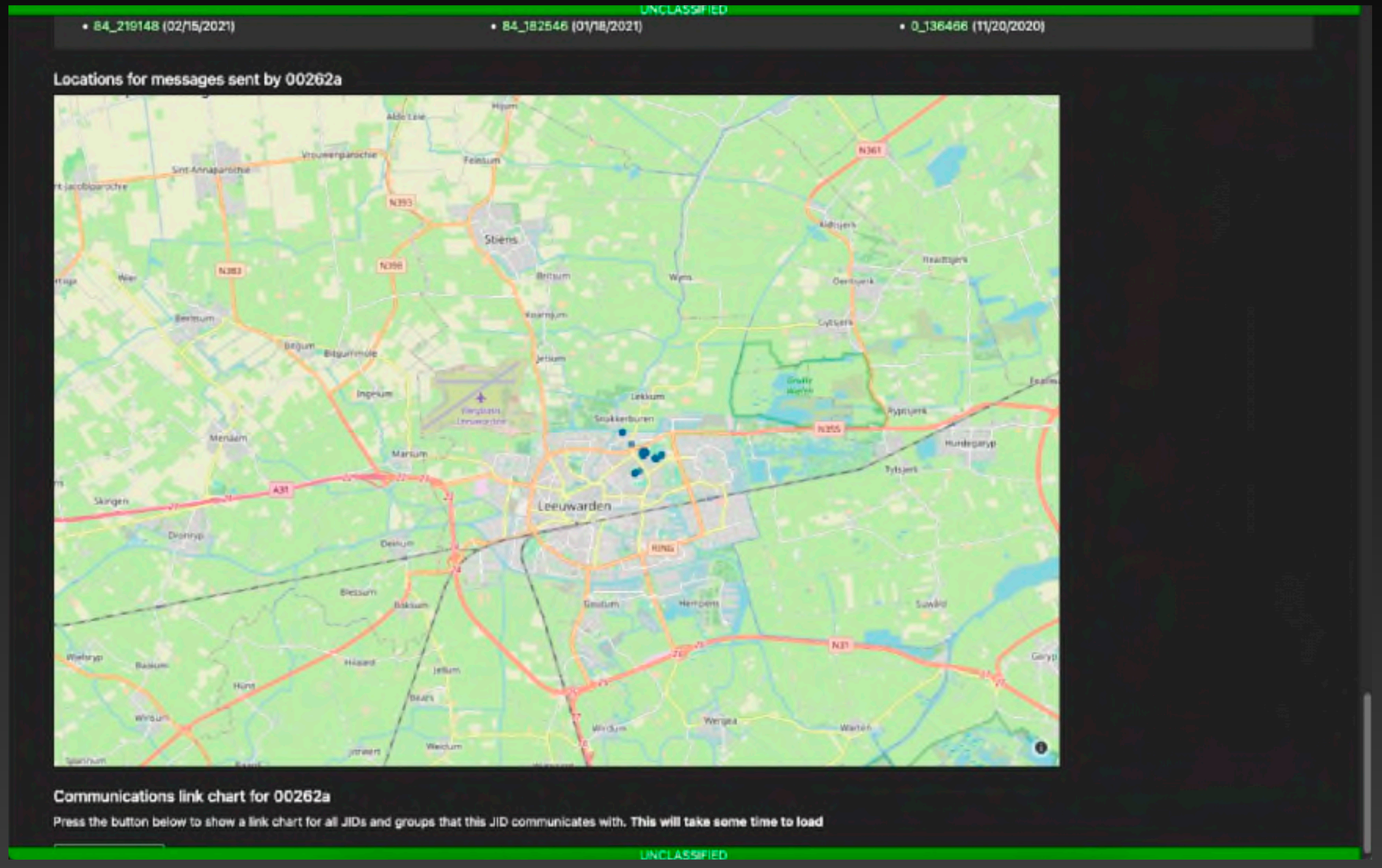
The Interface

HolaiBot

● PRIV								
● PERT ● NPERT ● PRIV	2	2021-03-15 07:12:55	286 - TR	mostlyinto	OG 👊	Haben wir eine Halle wo wir heute abladen könnten	39.0	1.615792363E1
● PERT ● NPERT ● PRIV	3	2021-03-15 07:15:12	286 - TR	mostlyinto	OG 👊	0:00 / 0:00 Update	39.0	1.615792363E1
● PERT ● NPERT ● PRIV	4	2021-03-15 07:16:12	286 - TR	mostlyinto	OG 👊	0:00 / 0:00 Update	39.0	1.615792363E1
● PERT ● NPERT ● PRIV	5	2021-03-15 07:16:24	286 - TR	mostlyinto	OG 👊	0:00 / 0:00 Update	39.0	1.615792363E1
● PERT	6	2021-03-15	286	mostlyinto	OG 👊	Hast du neue wickr	39.0	1.615793212E1

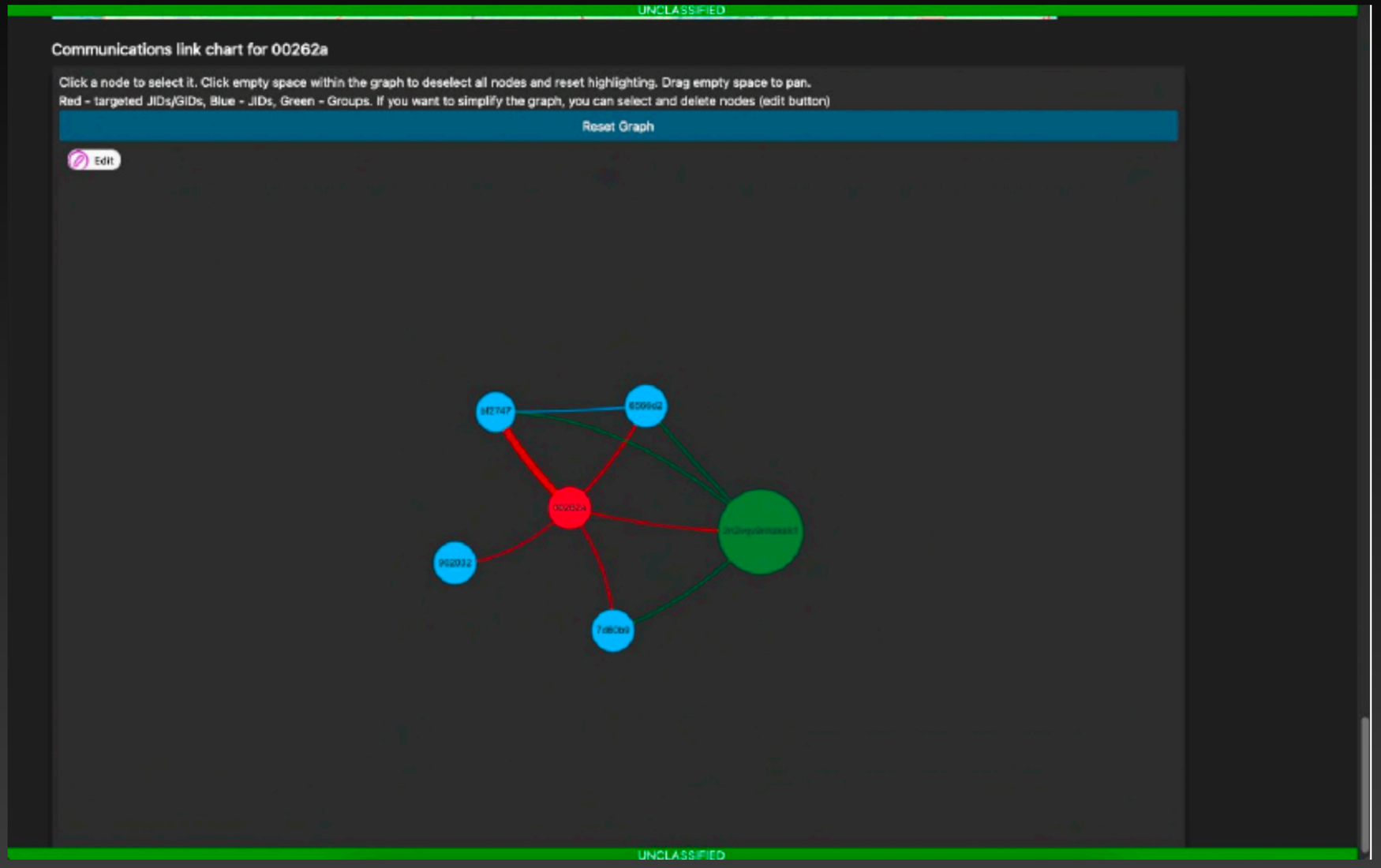
The Interface

HolaiBot



The Interface

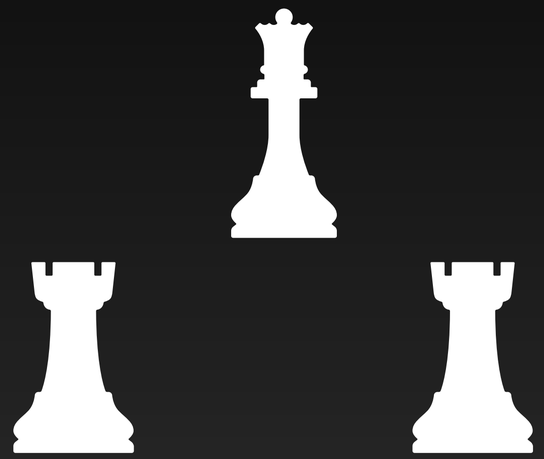
HolaiBot



The Structure of Anom



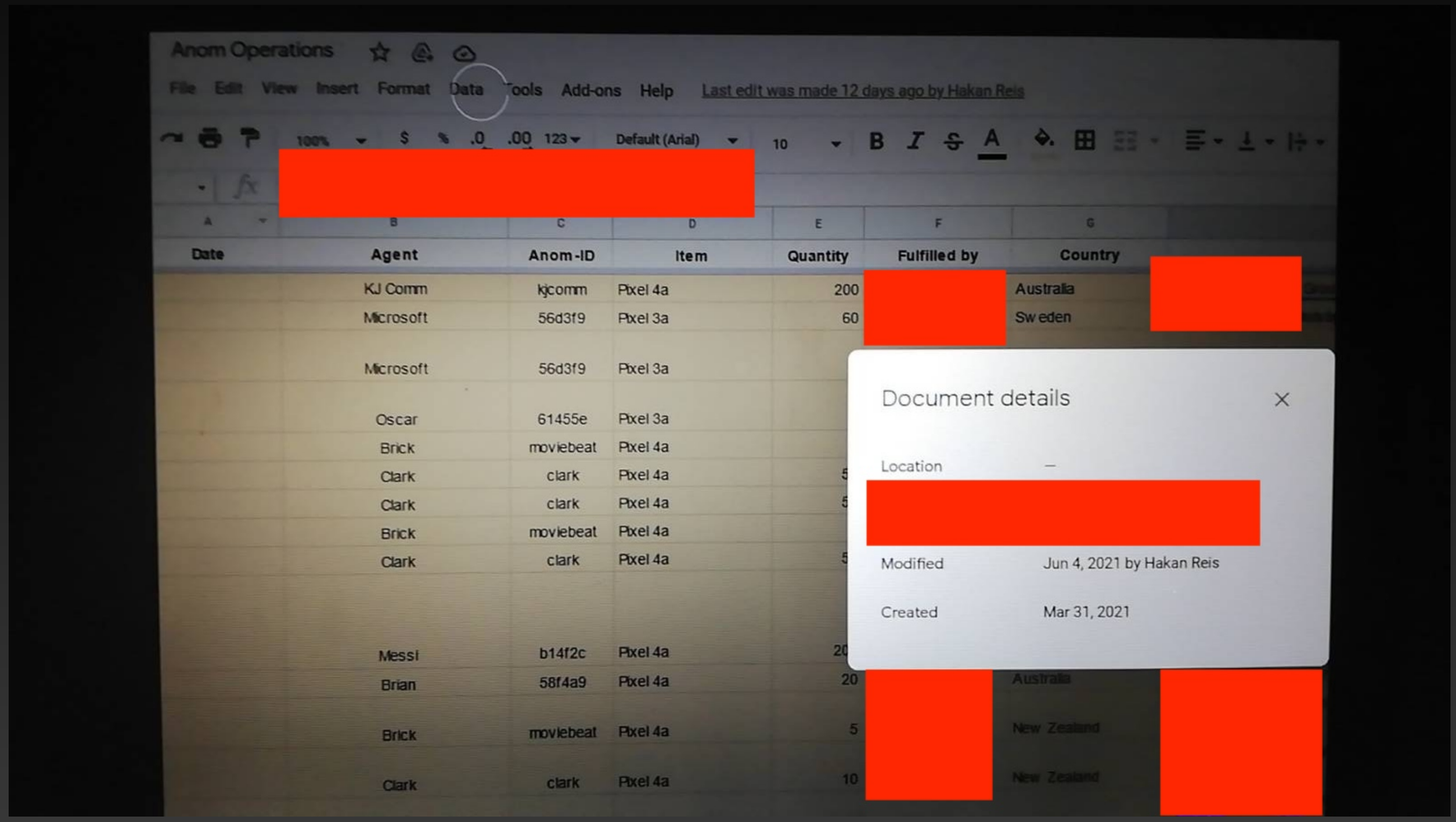




The Structure of Anom

The Top Distributors



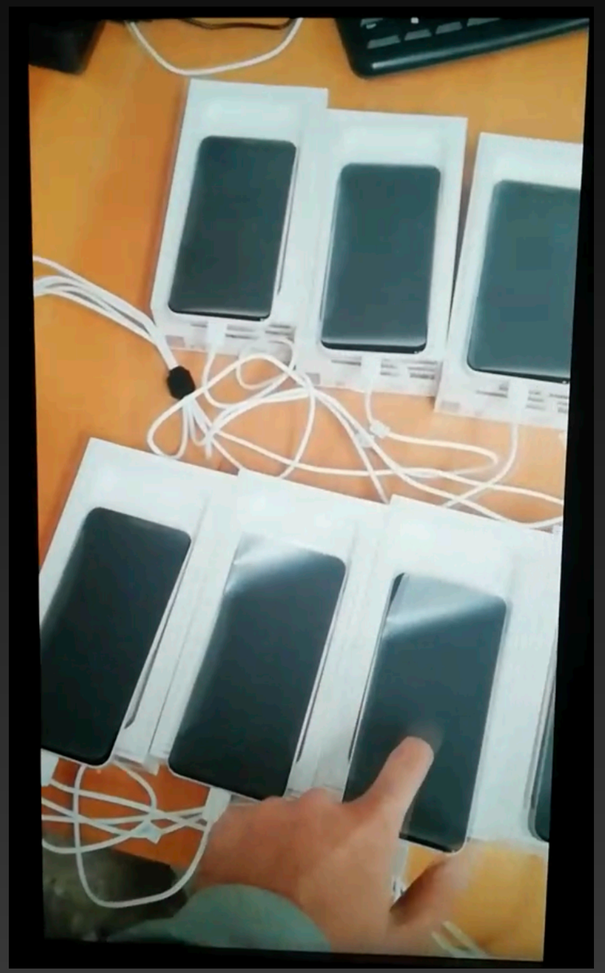




The Structure of Anom

The Resellers/Agents

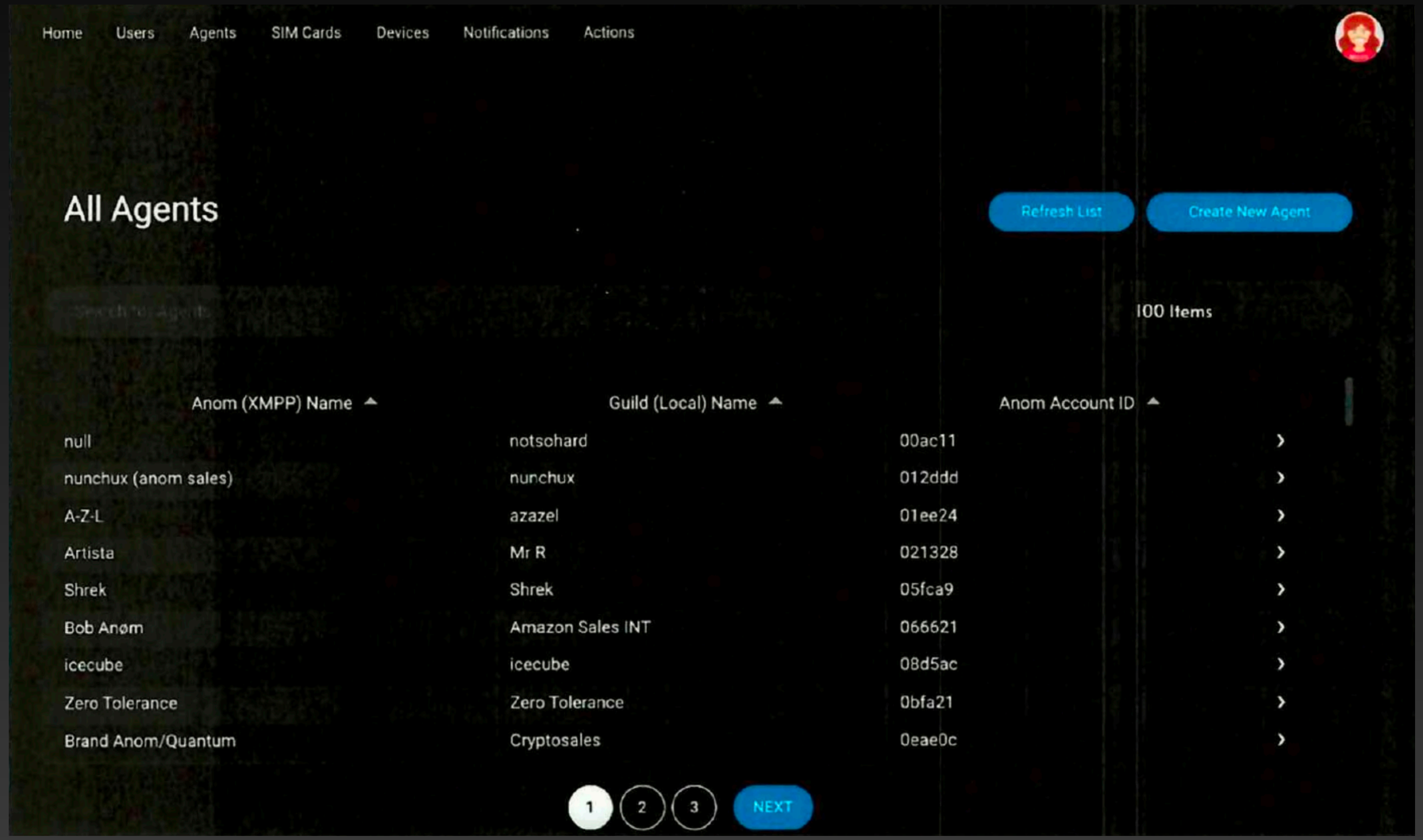






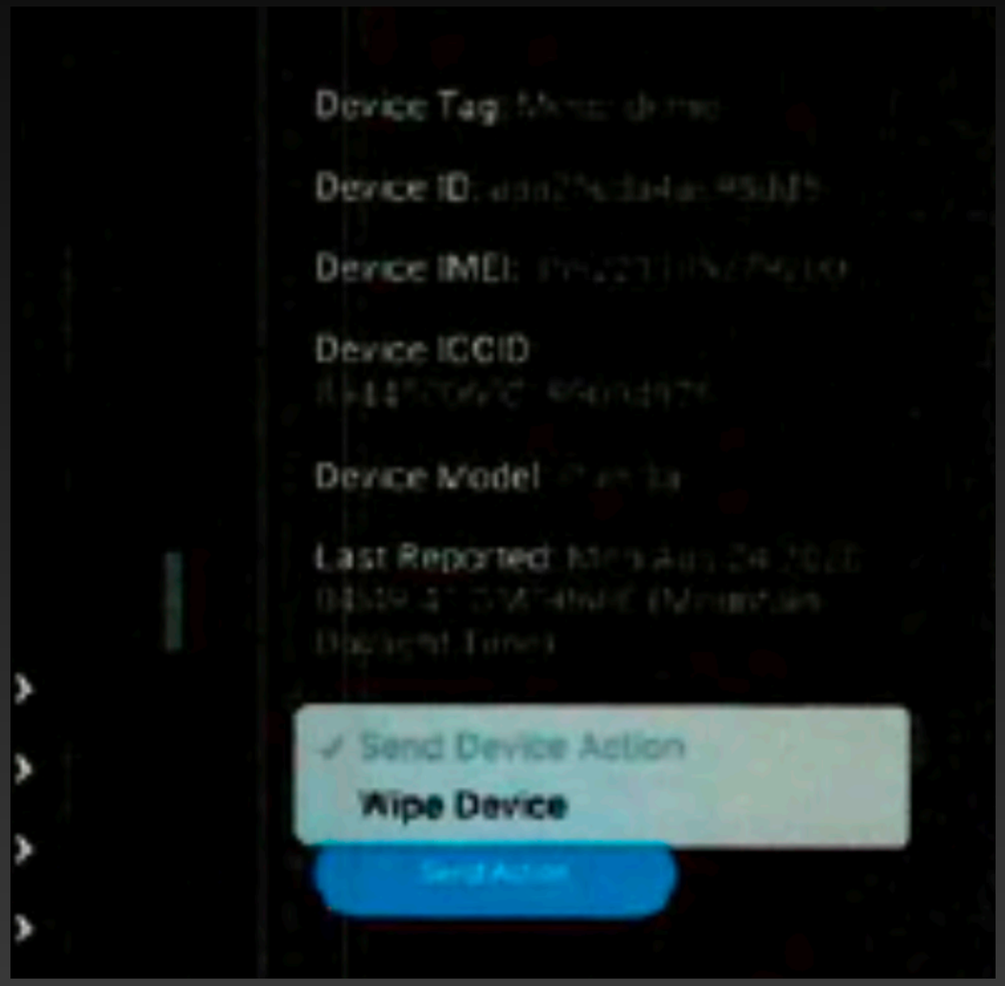
The Structure of Anom

The Resellers/Agents



The Structure of Anom

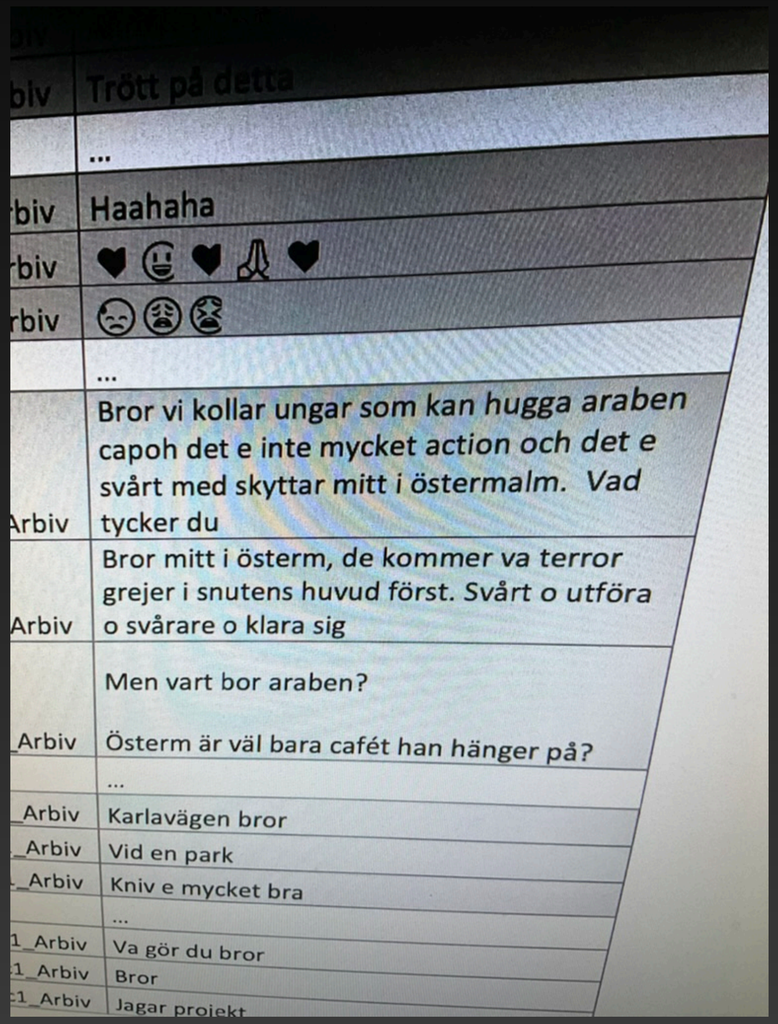
The Resellers/Agents



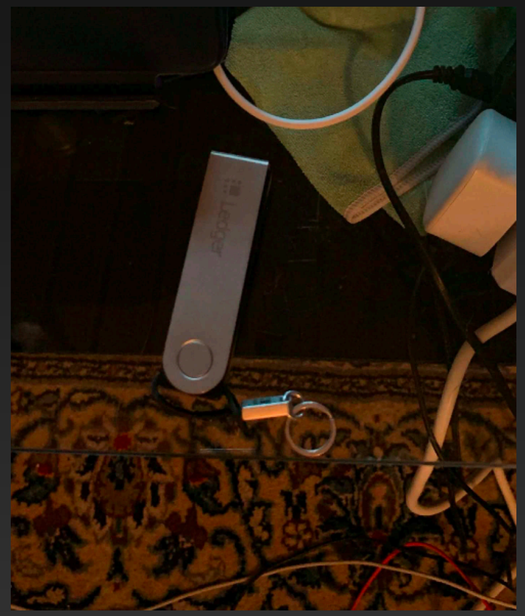


The Structure of Anom

The End Users



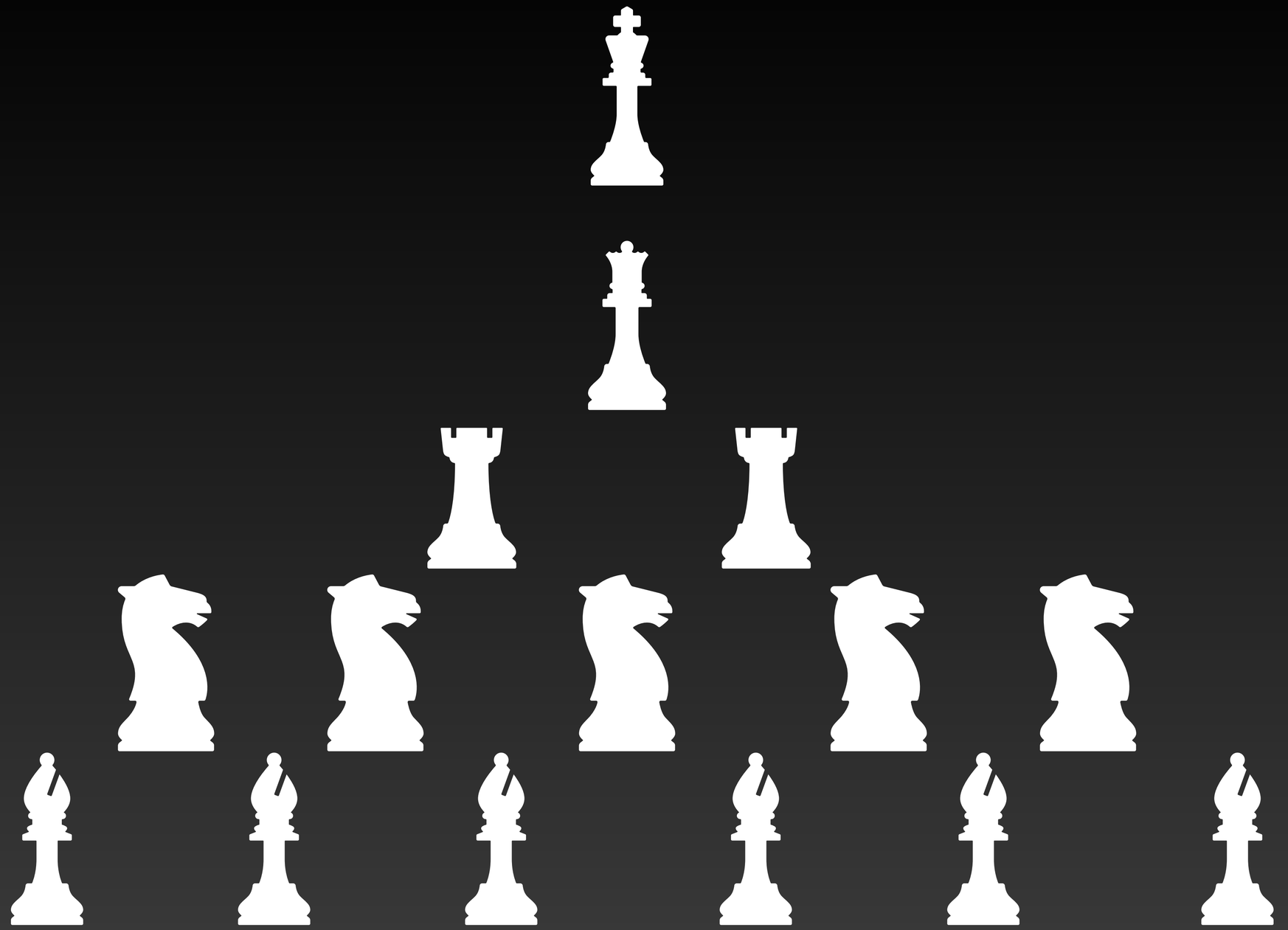


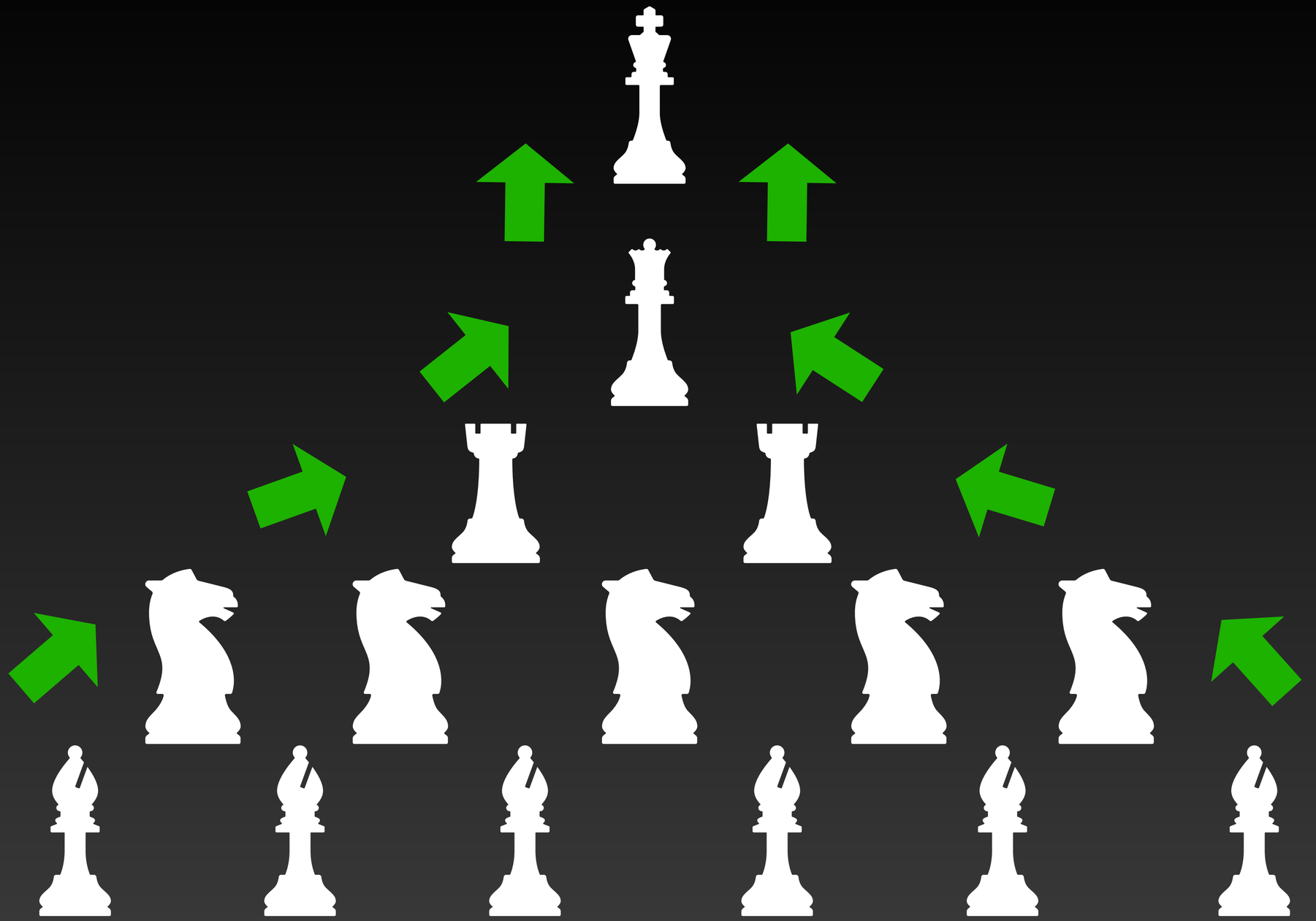






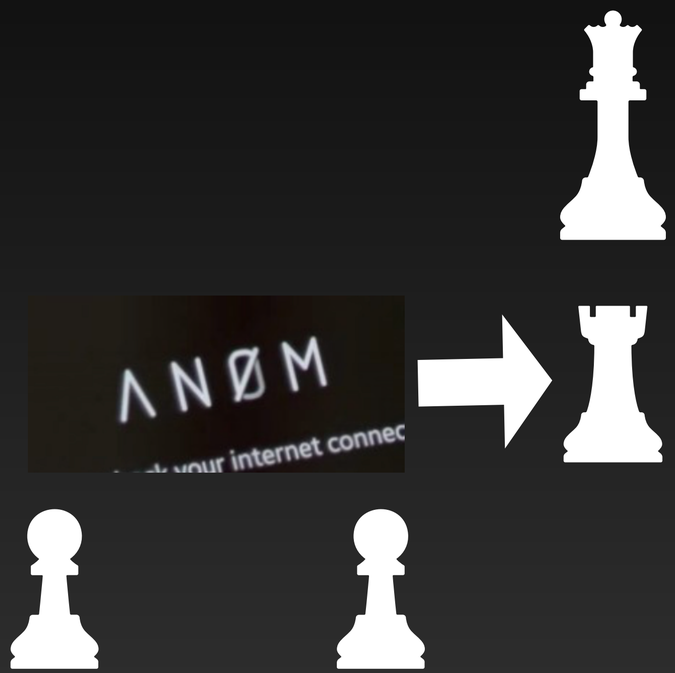


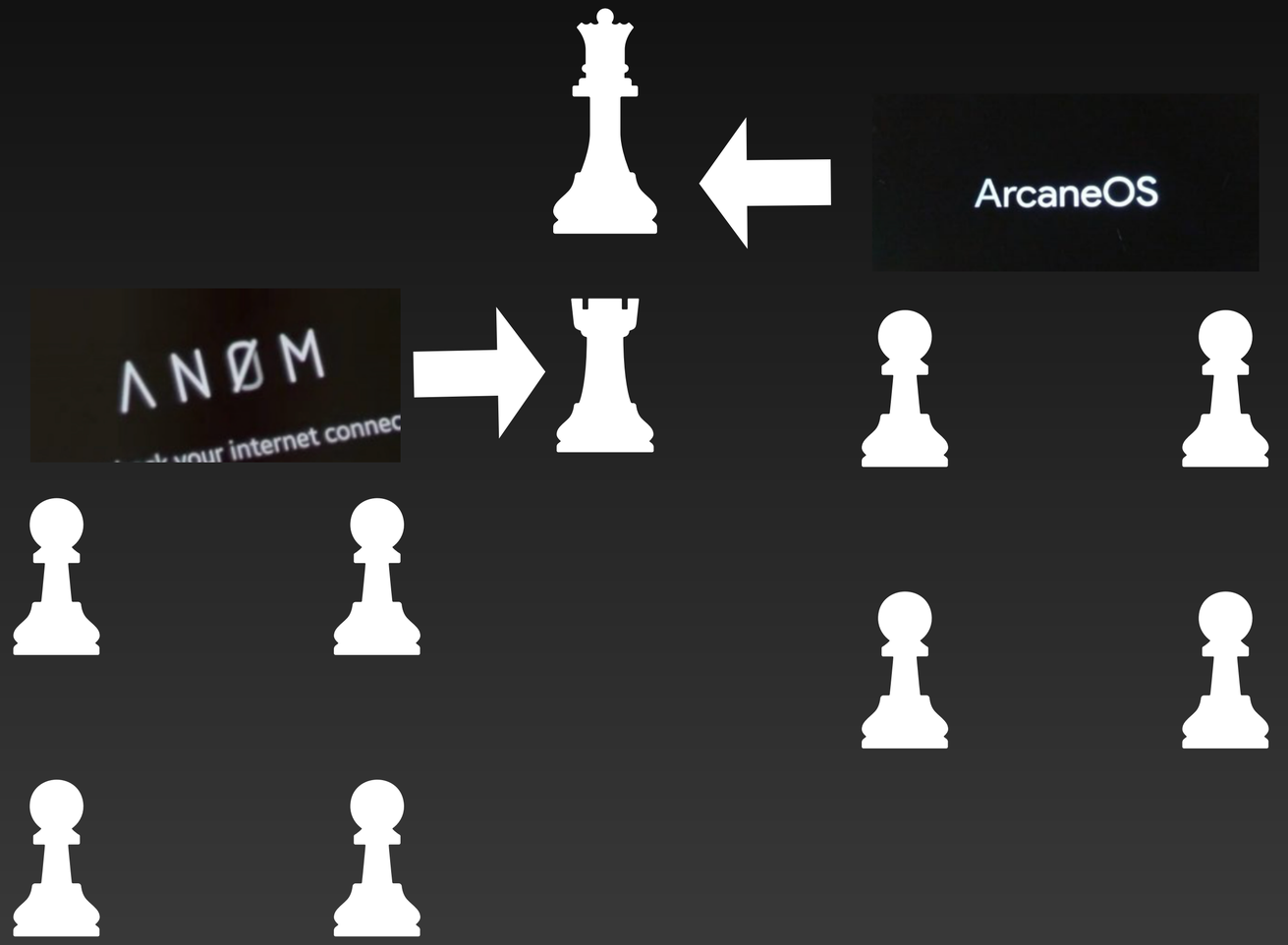









ANØM


ArcaneOS
ANØM

“Microsoft” and Black Boxes

(no relation to THAT Microsoft)



“Microsoft” and Black Boxes

Growth in Europe

Bundeskriminalamt

BKA

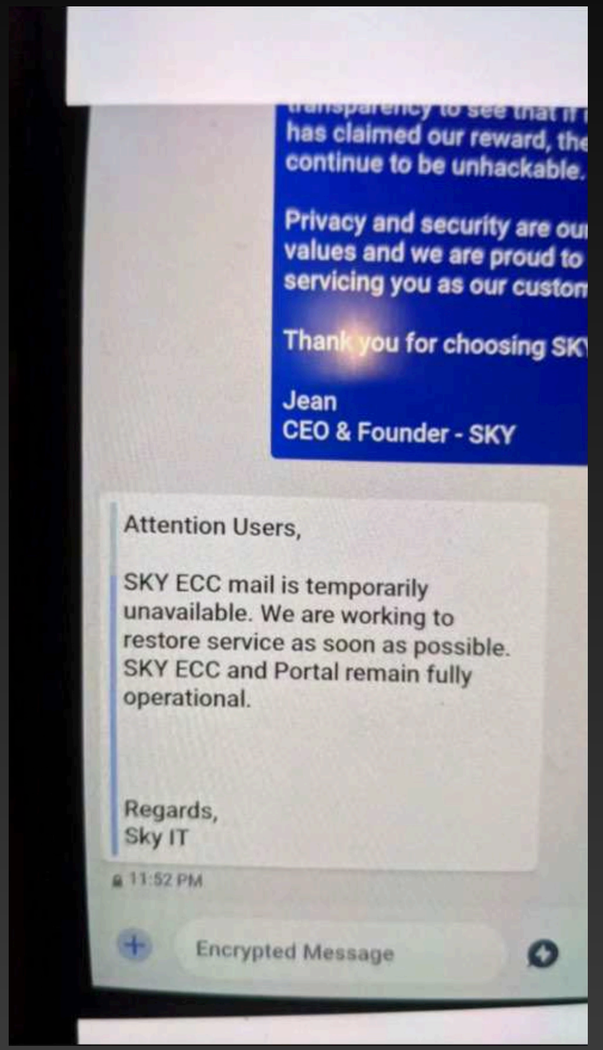
22.04.2020:

Am 22.04.2020 fand diesbezüglich eine Besprechung zwischen FBI und dem BKA statt.
Das FBI teilte hierbei mit, dass es in einem der genannten Ermittlungsverfahren gelungen sei, Teile der verschlüsselten Kommunikation über einen Server für kryptierte Kommunikation zu entschlüsseln und mit einem zwei- bis dreitägigen Zeitverzug zu erheben.
Zu diesem Zeitpunkt wurde dieser Server von zirka 10 Nutzern genutzt, von denen nach Einschätzung des FBI ca. 3 in Deutschland aufhältig waren.
Das FBI bot Deutschland an, Informationen mit Deutschland-Bezug zur weiteren Abklärung zu übermitteln.

“Microsoft” and Black Boxes

Sky Shutdown

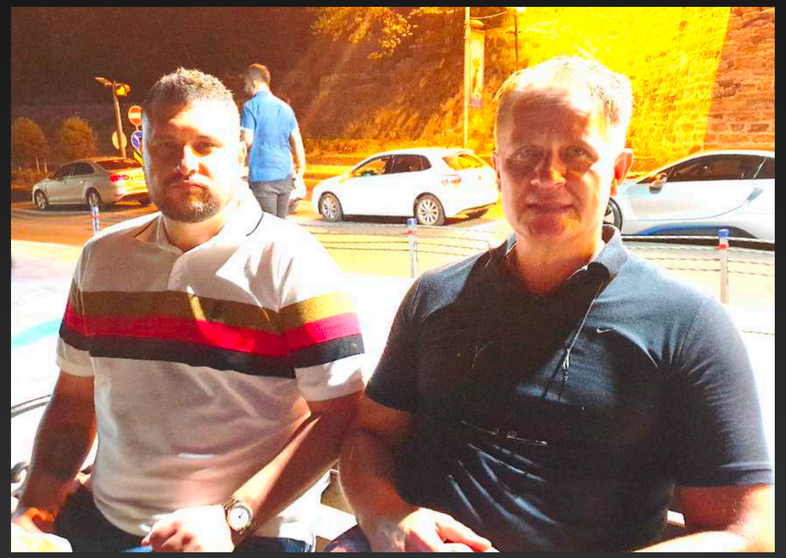




Push, push, push.

“Microsoft” and Black Boxes

Microsoft





“Microsoft” and Black Boxes

Microsoft





“Microsoft” and Black Boxes

The Office

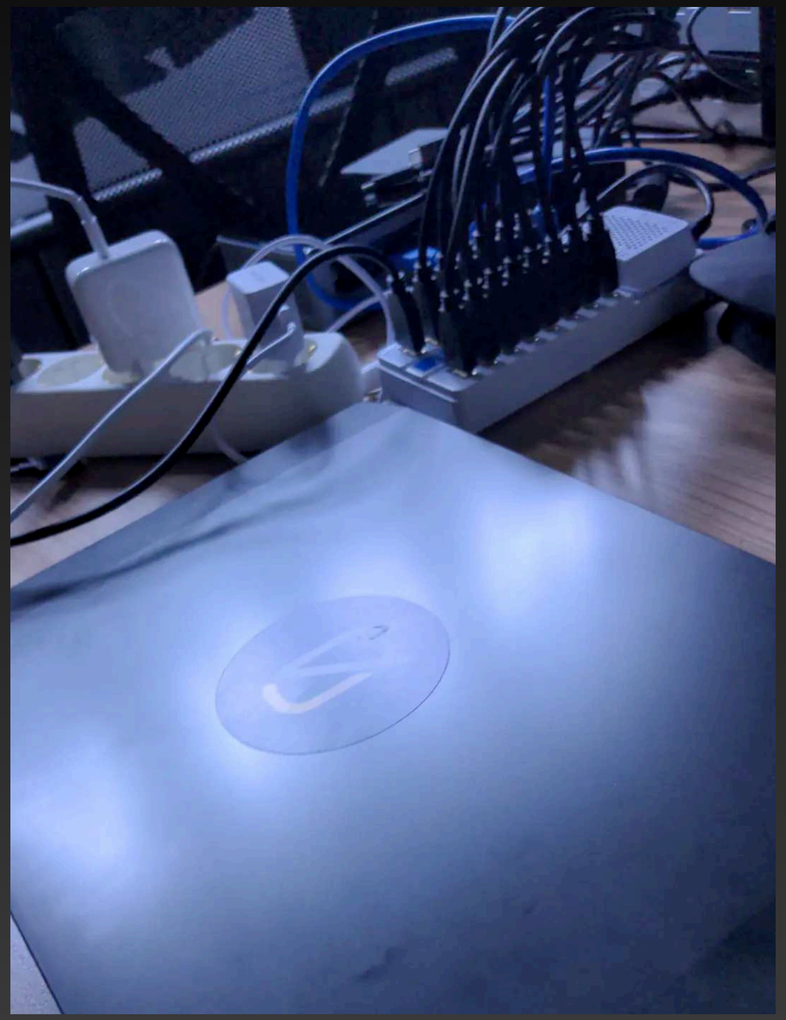


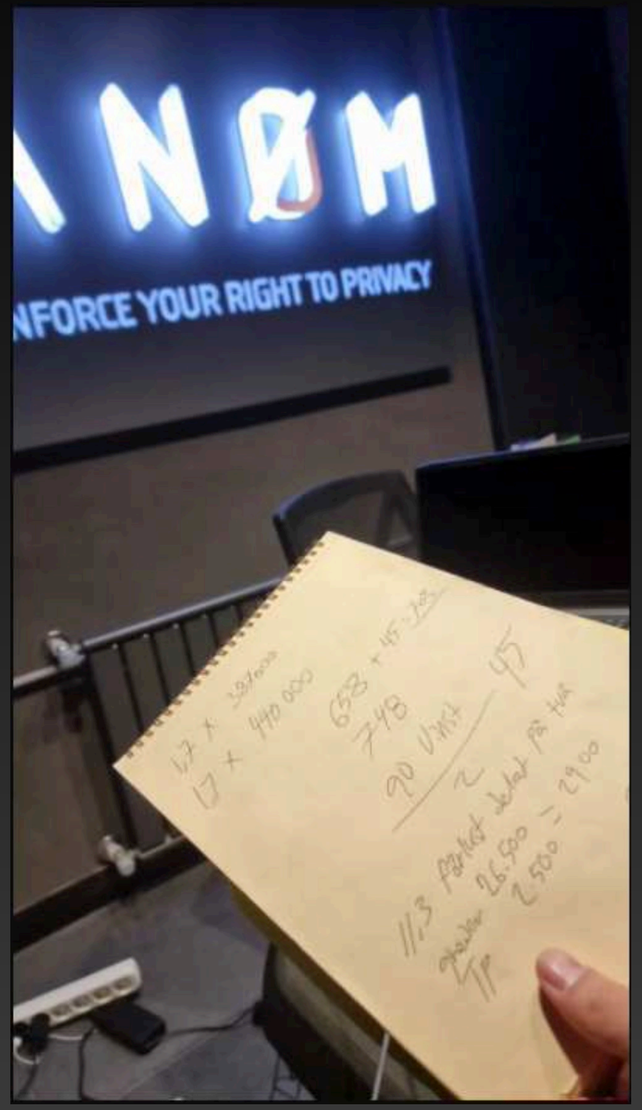


“Microsoft” and Black Boxes

The Office

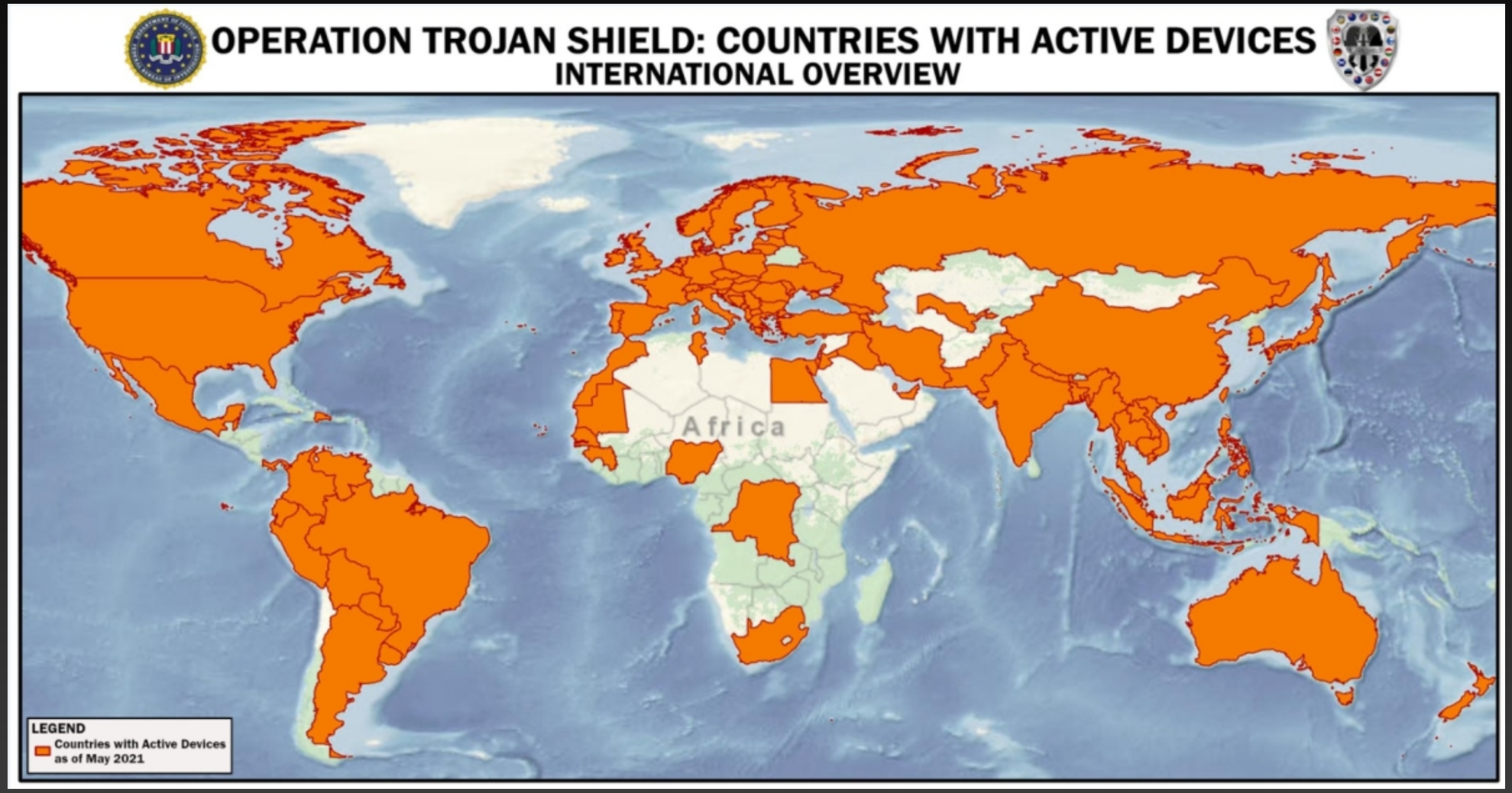






“Microsoft” and Black Boxes

Worldwide Growth



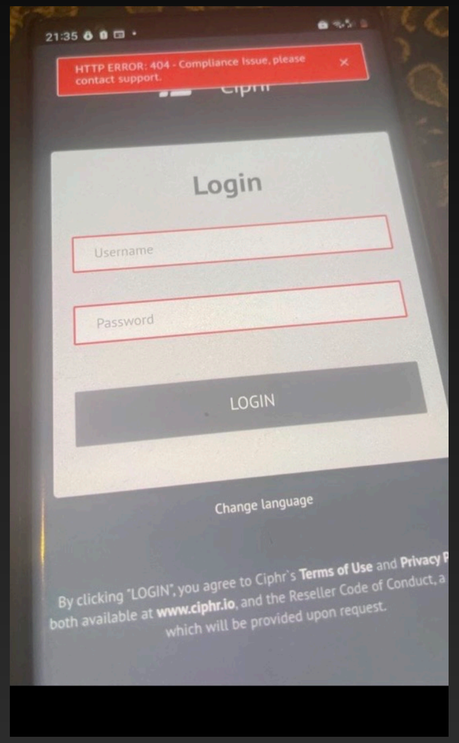
What This All Means for the Going Dark Debate

(the FBI will do this again)



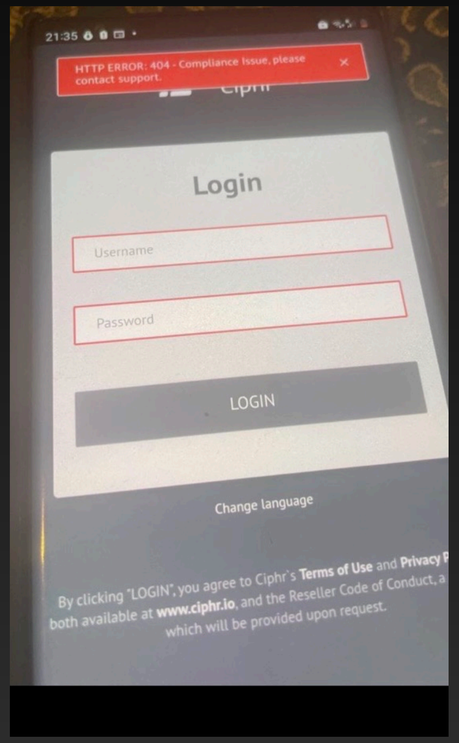
The Going Dark Debate

Shattered Trust



The Going Dark Debate

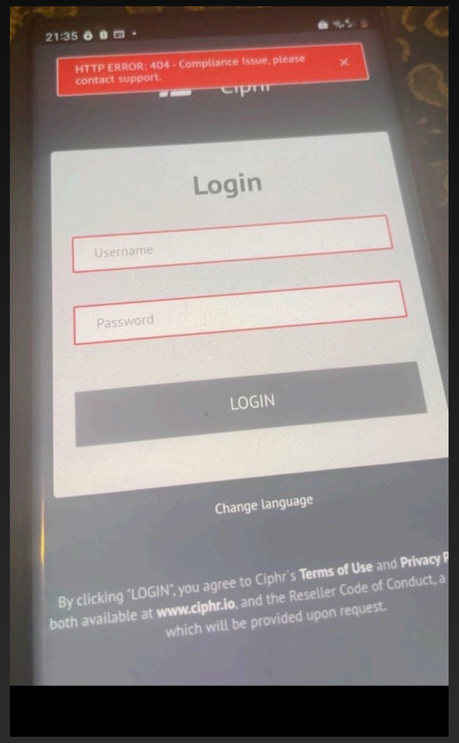
Shattered Trust





The Going Dark Debate

Shattered Trust









The Going Dark Debate

The Three Options

The Going Dark Debate

The Three Options

Front Door

- Apps give more data to law enforcement under legal order
- Will require holding more user data, undermining own security

The Going Dark Debate

The Three Options

Front Door

- Apps give more data to law enforcement under legal order
- Will require holding more user data, undermining own security

Back Door

- Law enforcement compromise entire chat platforms
- Has wide latitude for collateral surveillance

The Going Dark Debate

The Three Options

Front Door

- Apps give more data to law enforcement under legal order
- Will require holding more user data, undermining own security

Back Door

- Law enforcement compromise entire chat platforms
- Has wide latitude for collateral surveillance

Targeted Hacking

- Relies on an (expensive) market of exploits and offensive tools
- Can be crafted to only collect certain information on specific targets

The status quo is not sustainable

The status quo was what lead to Anom

404 MEDIA

404media.co

