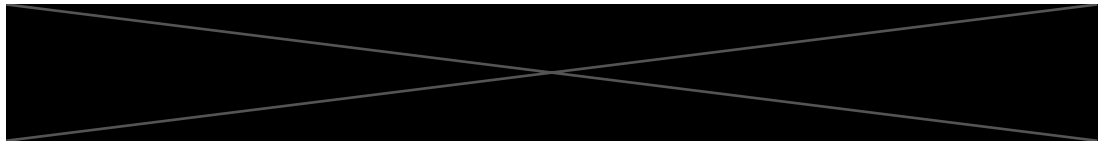
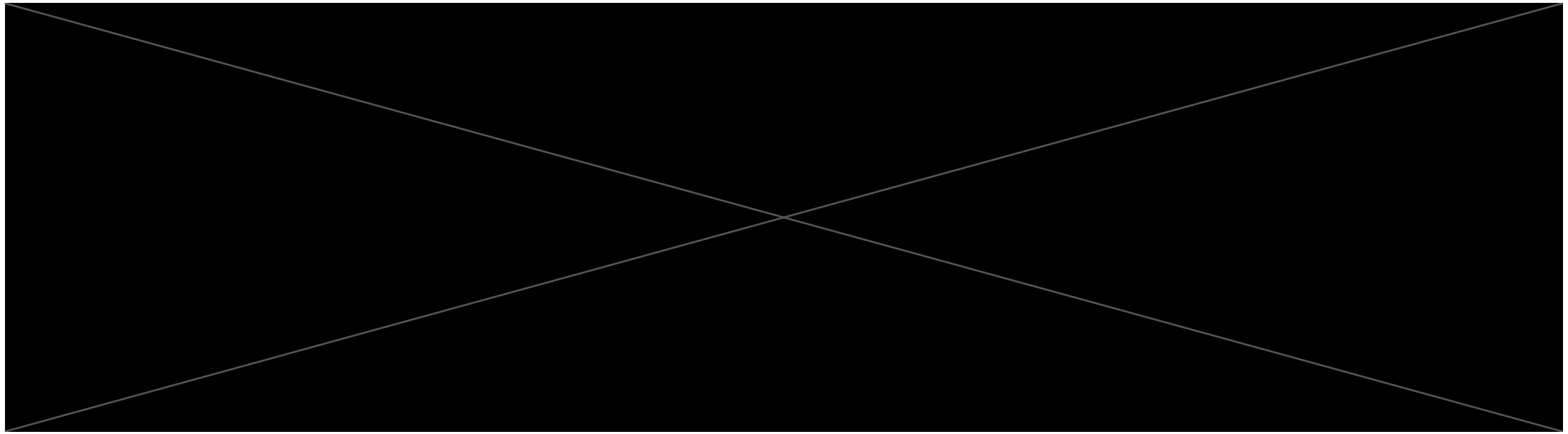
How do you do, fellow threat actors?



About me



Before we start

- TLP:AMBER, except when it's not
- This talk isn't what I planned for it to be
    - We're at, roughly, v37
    - This might already be outdated (.. again)
- I might breathe a bit oddly at times

2022 has been *wild* so far!

The elephant in the room: Ukraine

- Tremendous focus on the war, especially on hybrid aspects
- A *lot* of reporting included it, sometines unnecessarily
- To make this clear: Слава Україні!

There's a reason for that.

- First conventional war between European states since WW2
    - I'm aware of the Cod War, the Turkish Invasion fo Cyprus, Transnistria, ..
- First conventional war where we could expect to see hybrid operations that involve "cyber"
    - I'm aware of the 2006 Israel - Hezbollah war, the Houthi - Saudi war, ..
- In a sense: First proxy war since the collapse of the Soviet Union
    - I'm aware of the Syrian Civil war, ..

Everybody was waiting for the "big bang"

- Nervous European governments, especially in the beginning
- A lot of media attention, with a focus on critical infrastructure / energy sector
- And we waited, and waited, .. and still wait.

But why?

- Because subtle attacks are more useful
  - e.g. destroying communication channels vs. compromising them
  - Those have happened. A lot.
- Destructive attacks aren't politically opportune
  - And for Ukraine they are only somewhat necessary
  - See the events of the past couple of weeks
- Russia lack the capabilities
  - Typical targets invested in hardening measures
  - The "Russian playbook" for targeted CNO is pretty well known
  - Significant "brain drain" after February 24th / September 21st

Nonetheless: {ಠ_ಠ}

- This fixation used up a lot of attention and energy
- Threat actors noticed that - and acted on it
- Increased activity by some known actors since the war started ..

.. speaking of known

- Threat actor breached European governments and media agencies last fall
- Exploit in Zimbra (CVE-2022-24682), escalation from there
- Previously unknown threat actor TEMP_HERETIC

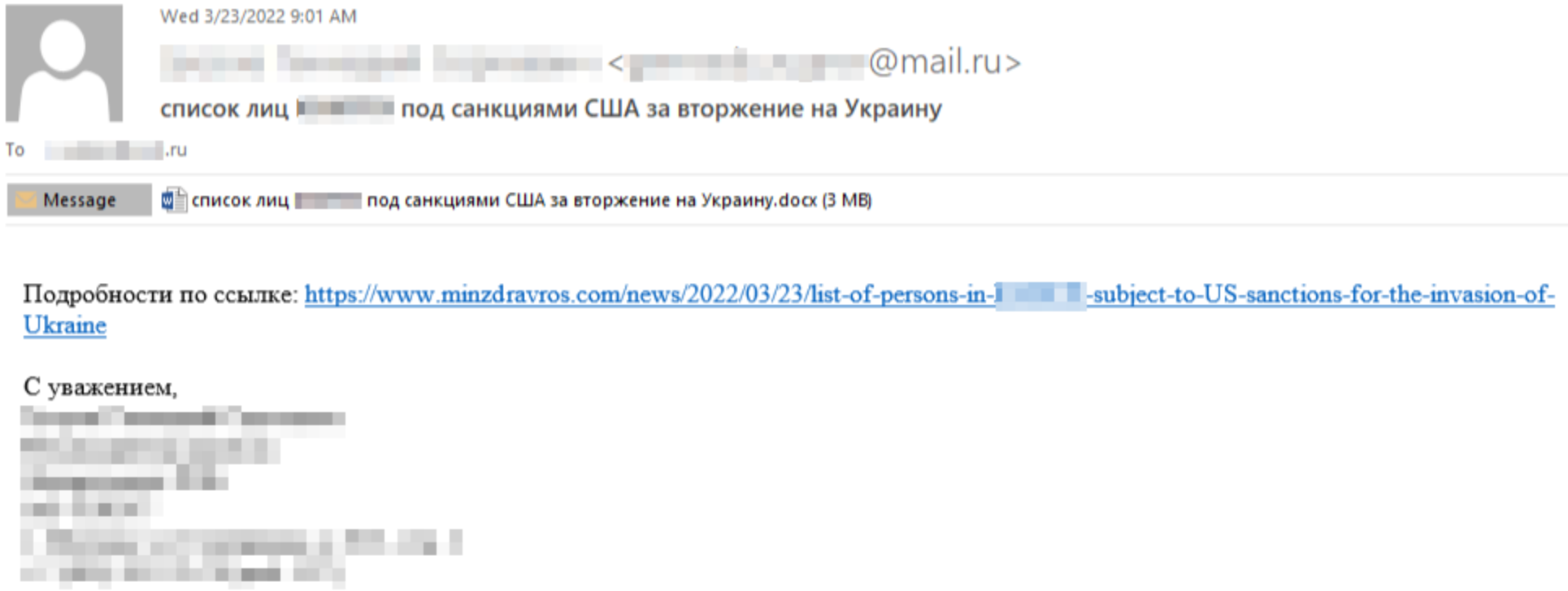
A few ~~eternities~~ months later ..

- Threat actor breached significant amounts of Zimbra installations again
- This time: Government systems on a mostly regional level in UA, RU, BY
- No attribution, but this happened in January '22 - before publication
    - High confidence that this was TEMP_HERETIC - China.

My war brings all boys to the yard

- Ties into other operations starting shortly before the invasion in February
- Mails with a pretext surrounding the conflict situation were sent before, ..

.. and after the war began



Wed 3/23/2022 9:01 AM

[redacted]@mail.ru>

список лиц [redacted] под санкциями США за вторжение на Украину

To [redacted].ru

Message список лиц [redacted] под санкциями США за вторжение на Украину.docx (3 MB)

Подробности по ссылке: https://www.minzdravros.com/news/2022/03/23/list-of-persons-in-[redacted]-subject-to-US-sanctions-for-the-invasion-of-Ukraine

С уважением,

[redacted]

War - What is it good for? (Espionage)

- Excellent pretext for malicious mails in a defense context
- Chinese actors attacked Rostec Corporation, Indian actors targeted Pakistani targets
- Iranian actors targeted critical infrastructure in Israel - keep that in mind

Speaking of Iran .. another elephant!

- July 18th: Albanian government (services) temporarily shutdown
- July 26th: Claim of responsibility by "HomeLand Justice"
  - Reference of Durrës, a county hosting a conference by MEK
  - Continued leaks of Albanian government documents
- Technical details: Mandiant, and you're good
- Attributed to the Iranian state by both government and private entities

We good, right?

- Operations like this have happened for years
  - Destructivity rare, but not unseen
- Think of the Bundestag-Hack, the DNC-hack, Macron-Leaks, ..
- This is where it usually ends. Usually.

Prepare for trouble & make it double

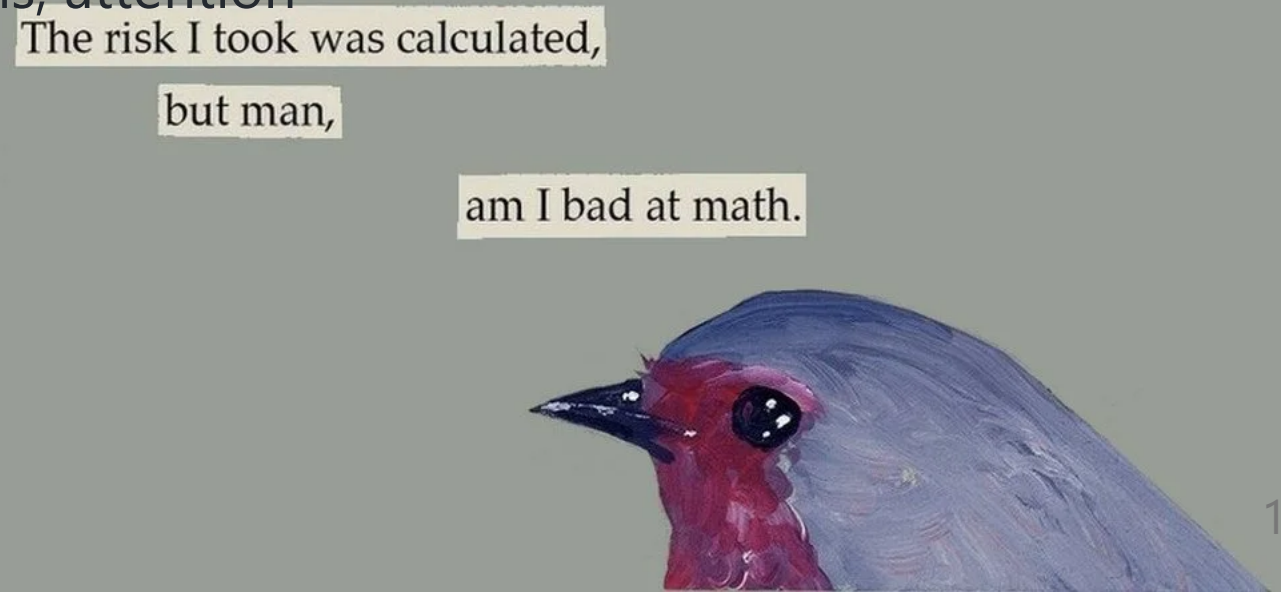
- Albania was hit once again at the beginning of September
- Traveller Information Management System (TIMS) was hit, causing issues at borders
- Potentially revenge for the public attribution?

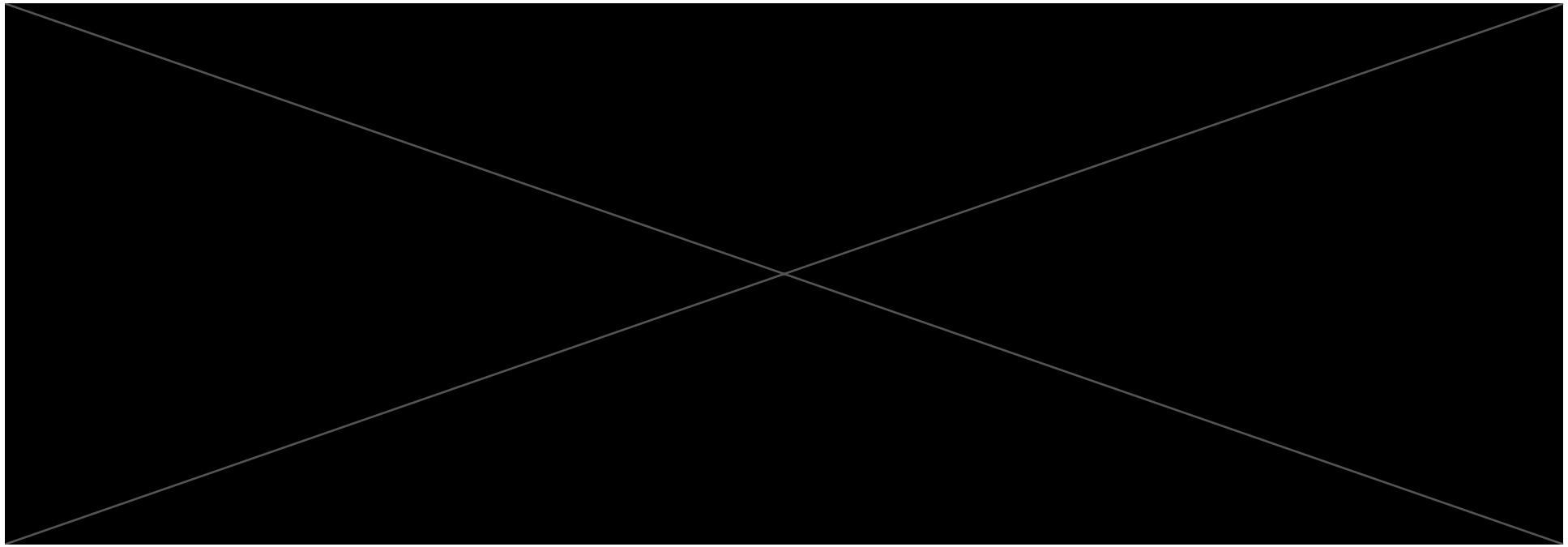
This blew up .. massively

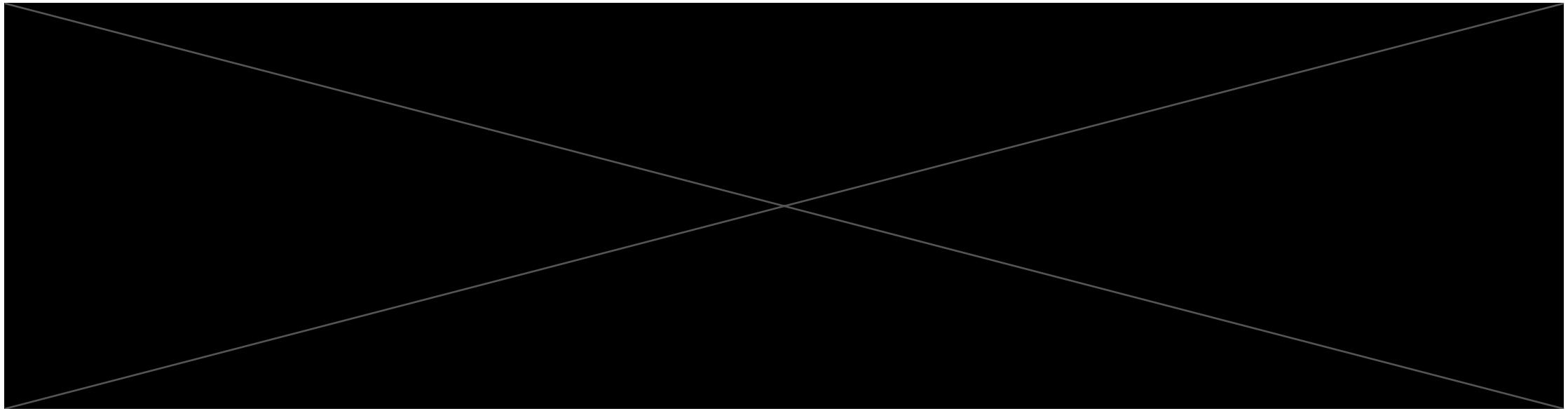
- Albania severed all diplomatic relations with Iran in September
    - First ever instance of this happening in response to a CNO
- Albania demanded invocation of Article 5
    - Which caused quite a ruckus
- International partners (almost) unanimously stood behind Albania

Abort, abort, abort

- This was most likely not worth it for Iran
- Political cost, potential new sanctions, attention







That transition is *very* awkward.

Bird is the word!

- "Predatory Sparrow", potentially known as Indra before
  - I'm not going to try to spell out "Gonjeshke Darande"
- Active since at least spring '22
  - In their previous incarnation: since at least '19
- Most attacks had actual consequences beyond "computer ded lol"

They have indeed been preying on stuff

- Attacks against Iranian petrol supply stations, coincided with the anniversary of the 2007 "Rationing Riots"
- Leak of CCTV-footage from inside a notorious Iranian prison
- Destructive attacks against Iranian steel plants shortly after they were sanctioned by the US
    - incl. leaking of data
- Attacks against Iranian railway systems

Safety first!

- There is some evidence that attacks have been ongoing since 2019
  - Possibly "getting their feet wet"?
- The attackers made sure that no people were harmed
  - Including notifying authorities beforehand

Who are the birdmen?

- Checkpoint says it's unlikely that it's a state-sponsored actor
    - Surprise: I disagree
- Their attacks were careful in their destructivity
- There was almost always messaging
    - "Call the office of the Supreme Leader"

We don't know.

Interesting theory about birds

What's the point of all of this?

Some significant things ..

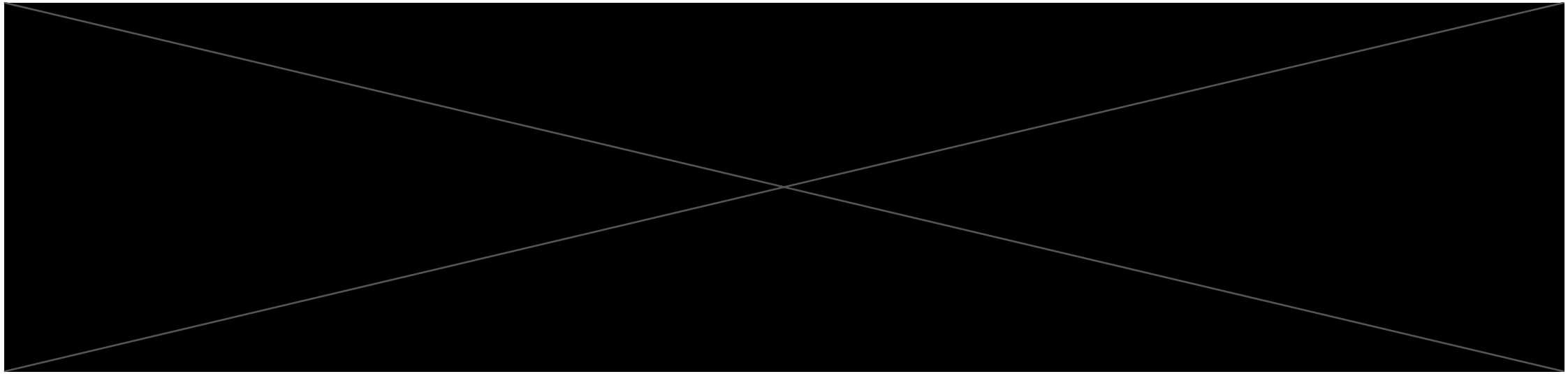
- Predatory Sparrow -> "responsible offensive computer network operations"
- Iran vs. Albania -> "new norms with regards to response to attacks on NATO members"

.. and much more happened

- We shouldn't ignore Russia
    - We probably should ignore Killnet though
- We also very much shouldn't ignore other threats
- Ignoring other bad actors isn't helping Ukraine
    - Keeping our systems safe is

I'm sorry. Kind of.

- What I planned: Information about barely known stuff.
- What I accomplished: Giving you a recap of the year (so far).
    - Which is a lot, some unprecedented, but still
- The singular point I'm trying to make is: Don't lose focus.



Questions?

&

Obligatory dog: