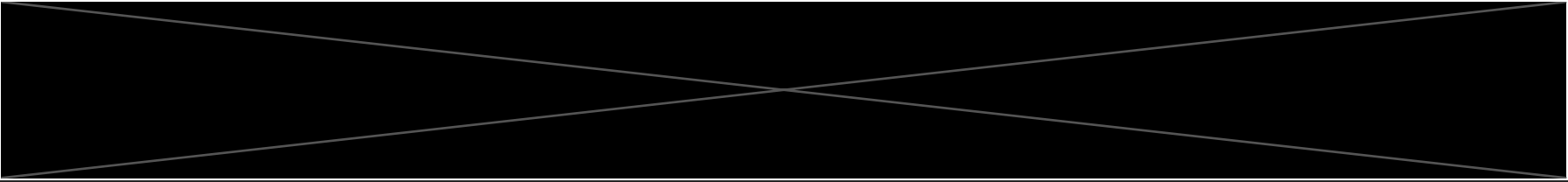
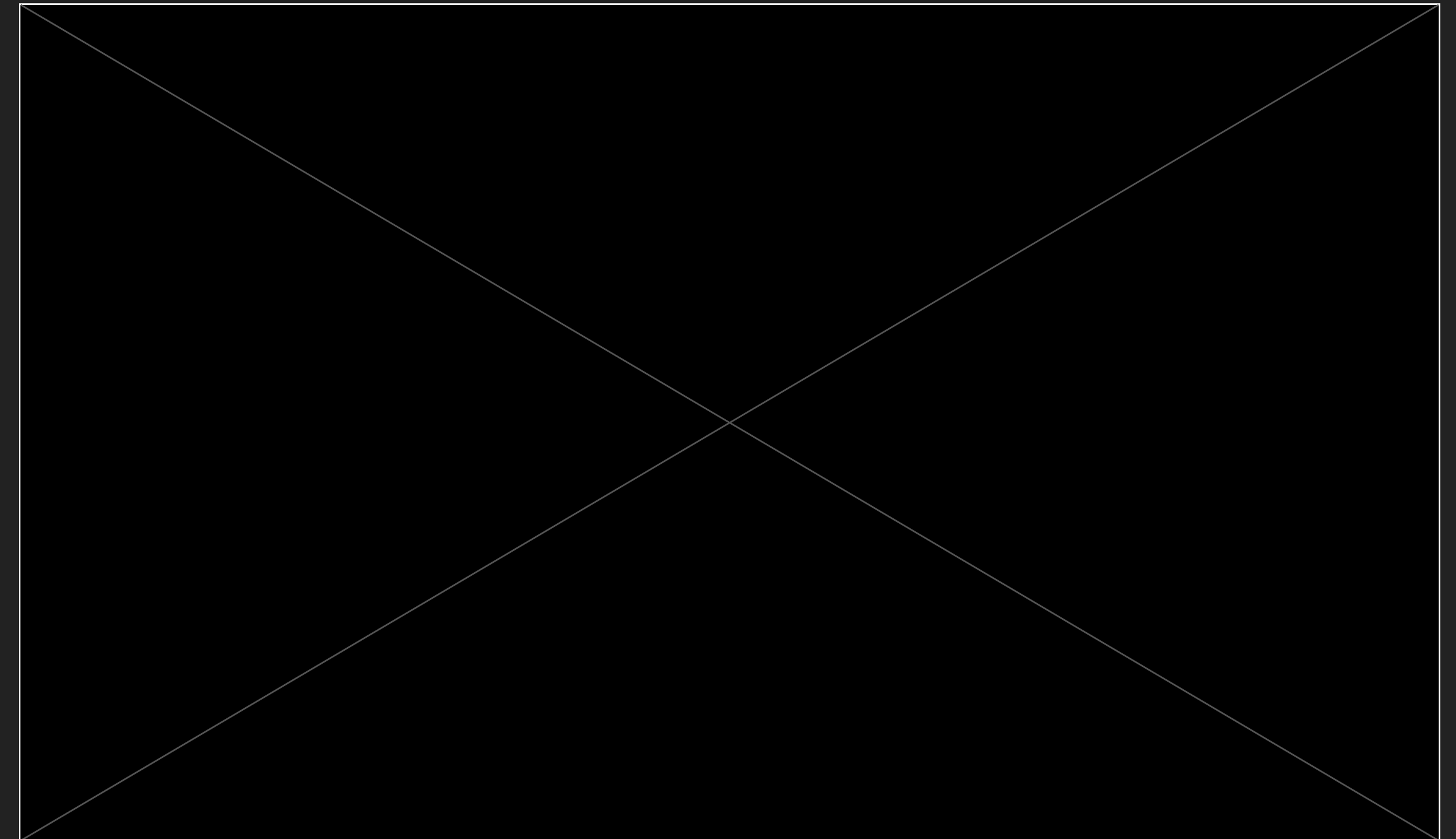


FROM BORSCHT TO BYTES

THE FUSION OF RUSSIAN INTEL AND CYBERCRIME

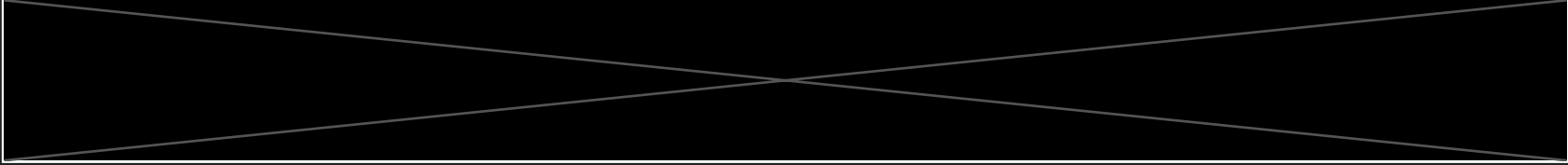
WHO AM I?

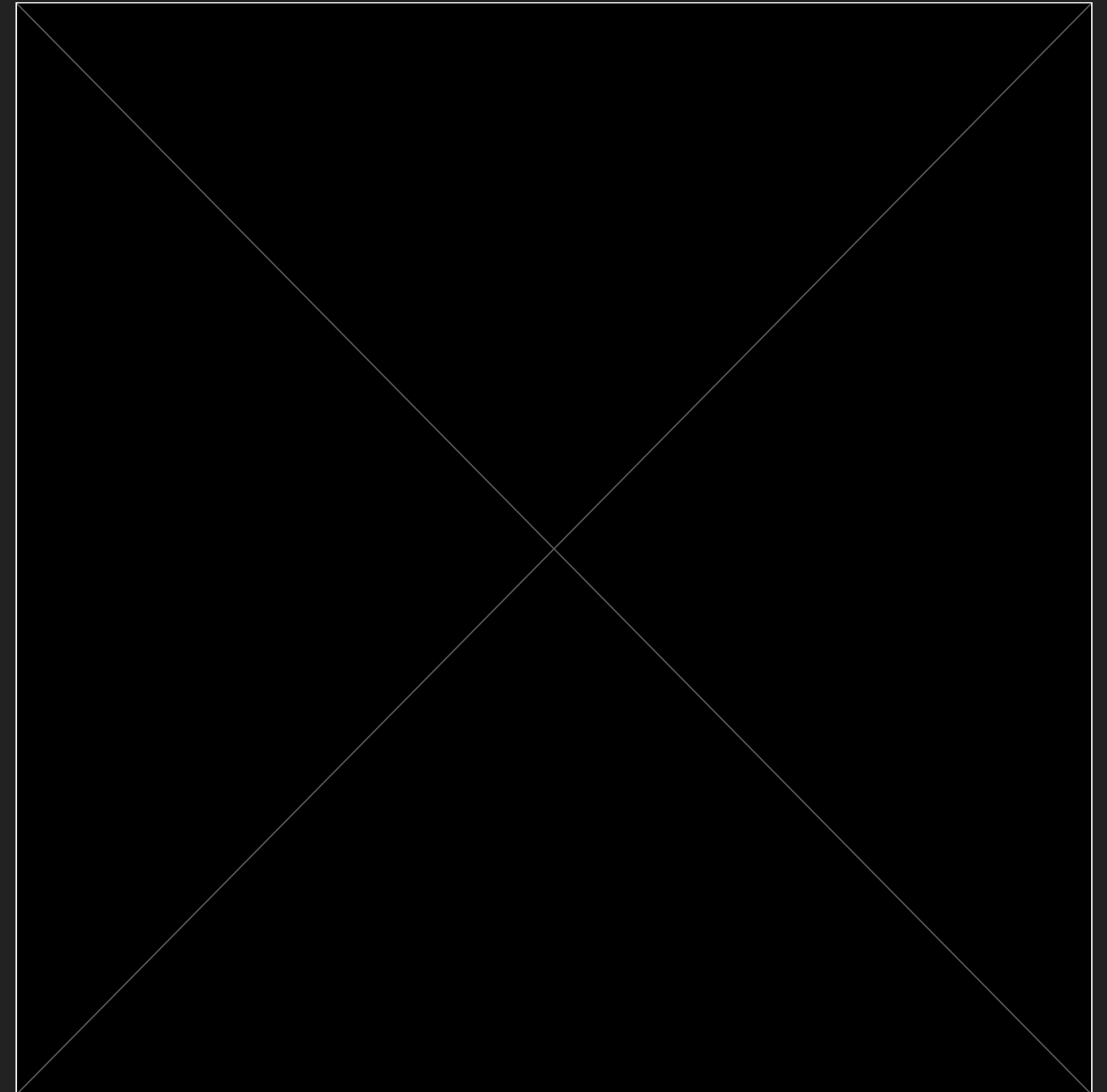
- ▶ 
- ▶ DFIR → CTI
- ▶ Unfortunately: I'm okay-ish @ DFIR.
- ▶ Fortunately: I like books.
- ▶ Fortunately: Times are changing.



[TLP:AMBER]

WHO AM I?

- ▶ 
- ▶ DFIR → CTI
- ▶ Unfortunately: I'm okay-ish @ DFIR.
- ▶ Fortunately: I like books.
- ▶ Fortunately: Times are changing.



INFOSEC HAS CHANGED

- ▶ We all remember APT1
- ▶ Old narratives are bullshit
 - ▶ “Russians steal money, Chinese technology”
- ▶ Cybercrime is everywhere
- ▶ Cybersecurity is (part of) statecraft
 - ▶ .. and so is cybercrime, in a way

INFOSEC HAS CHANGED

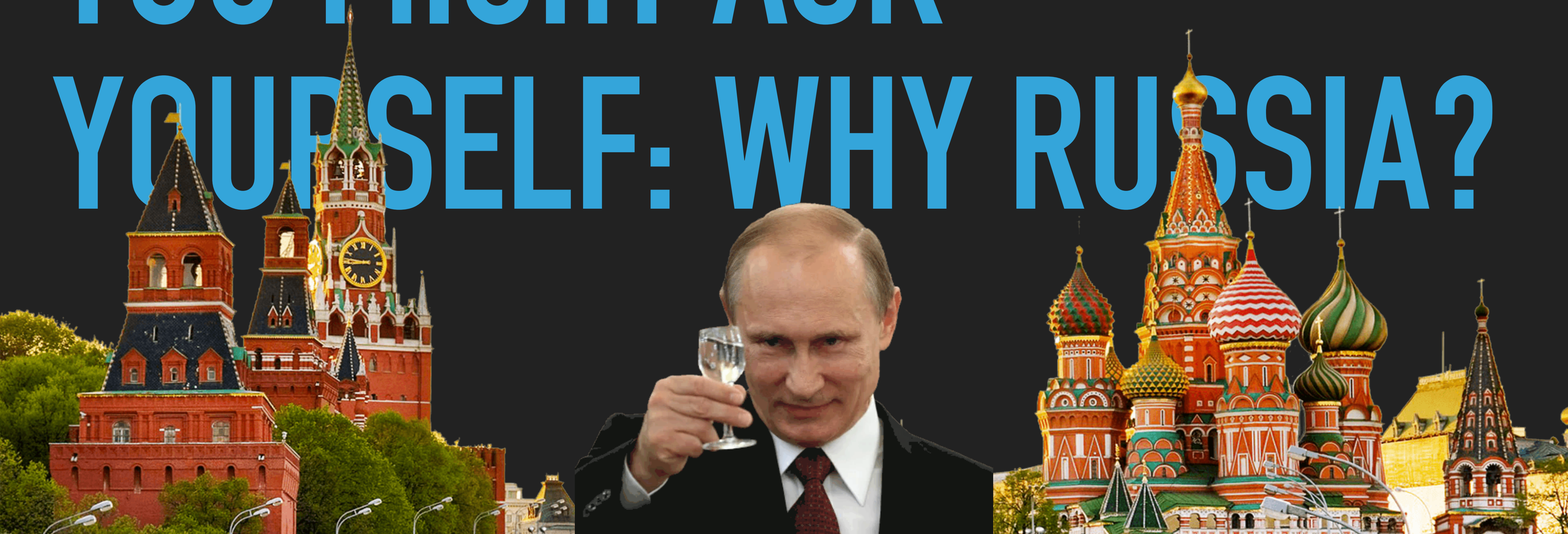
- ▶ We all remember APT1
- ▶ Old narratives are bullshit
 - ▶ “Russians steal money, Chinese technology”
- ▶ Cybercrime is everywhere
- ▶ Cybersecurity is (part of) statecraft
 - ▶ .. and so is cybercrime, in a way



YOU MIGHT ASK

YOURSELF: WHY RUSSIA?

**YOU MIGHT ASK
YOURSELF: WHY RUSSIA?**



WHY RUSSIA(N-LANGUAGE) CYBERCRIME?

- ▶ It's huge, well-established and sophisticated
- ▶ Comparatively well-studied in the West
- ▶ Unique, or at least uncommon social dynamics

WHY RUSSIA(N-LANGUAGE) CYBERCRIME?

- ▶ It's huge, well-established and sophisticated
- ▶ Comparatively well-studied in the West
- ▶ Unique, or at least uncommon social dynamics
- ▶ ~~It keeps me employed~~
- ▶ It has a direct impact on my work
 - ▶ My Russian is better than my Mandarin. Barely.



WHAT MAKES IT SO SPECIAL?

WHAT M



CIAL?

TIME FOR A HISTORY LESSON

- ▶ Early Russian Federation lacks civilian telecommunication networks
 - ▶ Almost entirely Rostelekom owned phone lines - thanks KGB!
- ▶ Massive growth up to 2000; 6.6 million Internet users
- ▶ Little regulatory oversight, significant market arose



TIME FOR A HISTORY LESSON

- ▶ Research funding diminished by around 80%
 - ▶ Defense procurement vanished similarly
- ▶ Scientific brain-drain - or "brain-change"
 - ▶ STEM-education still strong, even today
- ▶ Expectations vs (market) realities



THE SECRET INGREDIENT IS CRIME

- ▶ Cybercrime is almost always financially lucrative
- ▶ Cybercrime is comparatively easy
 - ▶ Knowledge, target-rich environment, security that sucks ass
- ▶ Chaotic beginning, organized progress
 - ▶ Prime example: Ransomware-support

THE SECRET INGREDIENT IS CRIME

- ▶ Cybercrime is almost always financially lucrative
- ▶ Cybercrime is comparatively easy
 - ▶ Knowledge, target-rich environment, security that sucks ass
- ▶ Chaotic beginning, organized progress
 - ▶ Prime example: Ransomware-support



BUDAPEST ~~CONVENTION~~ SUGGESTION

- ▶ Russian Criminal Code is lenient for cybercrime
 - ▶ Russia never signed the Budapest Convention
- ▶ Enforcement? Selective at best
 - ▶ Barely there most of the time
- ▶ Speaking of the state ..

BUDAPEST CONVENTION SUGGESTIONS

- ▶ Russian Criminal Code is lenient for crime
 - ▶ Russia never signed the Budapest Convention
- ▶ Enforcement? Selective at best
 - ▶ Barely there most of the time
- ▶ Speaking of the state ..



A HISTORY OF (IN)CONVENIENCE



A HISTORY OF (IN)CONVENIENCE

- ▶ Bolsheviks starting out as bank robbers / with bank robbers
- ▶ Early Bolshevik regime press-ganging bandits
- ▶ NKVD relying on the “vorovskoi mir” in the Gulags
- ▶ Pimps and money changers used for espionage

A HISTORY OF (IN)CONVENIENCE

- ▶ Bolsheviks starting out as bank robbers / with bank robbers
- ▶ Early Bolshevik regime press-ganging bandits
- ▶ NKVD relying on the “vorovskoi mir” in the Gulags
- ▶ Pimps and money changers used for espionage



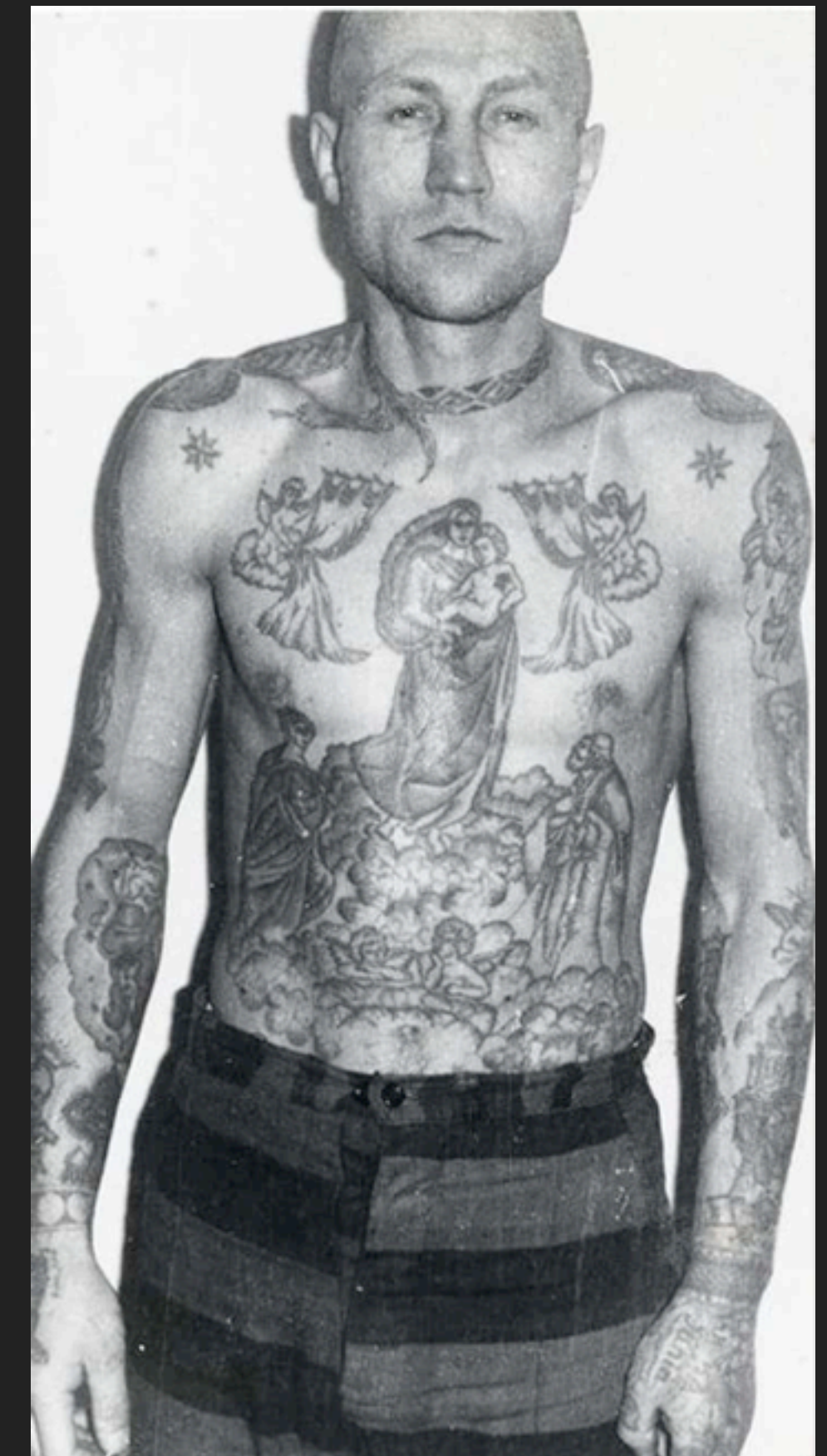
A HISTORY OF (IN)CONVENIENCE

- ▶ Bolsheviks starting out as bank robbers / with bank robbers
- ▶ Early Bolshevik regime press-ganging bandits
- ▶ NKVD relying on the “vorovskoi mir” in the Gulags
- ▶ Pimps and money changers used for espionage



A HISTORY OF (IN)CONVENIENCE

- ▶ Bolsheviks starting out as bank robbers / with bank robbers
- ▶ Early Bolshevik regime press-gangging bandits
- ▶ NKVD relying on the "vorovskoi mir" in the Gulags
- ▶ Pimps and money changers used for espionage



A HISTORY OF (IN)CONVENIENCE

- ▶ Bolsheviks starting out as bank robbers / with bank robbers
- ▶ Early Bolshevik regime press-gangging bandits
- ▶ NKVD relying on the "vorovskoi mir" in the Gulags
- ▶ Pimps and money changers used for espionage



A NEW WORLD, A NEW ORDER

- ▶ Fall of the Soviet Union, (temporary) fall of the KGB
 - ▶ Former assets became employers
- ▶ Putin turned, at least realigned the tables
- ▶ A lot of sticks, a lot of carrots
 - ▶ And: A lot of connections

A NEW WORLD, A NEW ORDER

- ▶ Fall of the Soviet Union, (temporary) fall of the KGB
 - ▶ Former assets became employers
- ▶ Putin turned, at least realigned the tables
- ▶ A lot of sticks, a lot of carrots
 - ▶ And: A lot of connections



COMINTERN? CRIMINTERN!

- ▶ Most people adopted, the state took care of the rest
 - ▶ Proscription 🤝 Prescription
- ▶ Not just in Russia - also in the diaspora
 - ▶ Intensified influence after 2014
- ▶ The same rules apply to all criminals
 - ▶ Even cybercriminals



SVR – THE “GENTLEMEN”

- ▶ External intelligence agency, civilian focus
- ▶ Espionage focus, both on- and offline
 - ▶ Can't not mention APT29
- ▶ Proud of their history, proud in general
 - ▶ Not the most popular folks



SVR – THE “GENTLEMEN”

- ▶ They keep their distance to the criminals
- ▶ Learning from reports about cybercrime
- ▶ Few examples of coercion / cooperation
 - ▶ Acquiring stolen credentials in '21
 - ▶ Using same exploits as Intellexa



GRU - THE BRAWLERS

- ▶ Military Intelligence / Counterintelligence
 - ▶ Better known for assassinations, sabotage
- ▶ APT28 (aka Fancy Bear), APT44 (aka Sandworm)
- ▶ Here, there, everywhere
 - ▶ MH17, OPCW, Tele5, NotPetya, ..
 - ▶ 🖐️ DSN



GU GRU - THE BRAWLERS

- ▶ Quite bullish at times, sometimes intentional
- ▶ “Whatever it takes”-approach
 - ▶ Adapting tools
 - ▶ Adapting techniques
 - ▶ ~~Adapting~~ Becoming criminals



**IF IT WALKS LIKE A
CRIMINAL ..**

BOTNETS ARE A GIRL'S BEST FRIEND *SING*

- ▶ 2018: VPNFilter is discovered
 - ▶ Malware targeting SOHO-devices
- ▶ 2022: Cyclops Blink is discovered
 - ▶ Same targeting, likely a replacement for VPNFilter
- ▶ 2024: Unnamed botnet is discovered
 - ▶ Same targeting, different method

BOTNETS ARE A GIRL'S BEST FRIEND *SING*

- ▶ 2018: VPNFilter is discovered
 - ▶ Malware targeting SOHO-devices
- ▶ 2022: Cyclops Blink is discovered
 - ▶ Same targeting, likely a replacement for VPNFilter
- ▶ 2024: Unnamed botnet is discovered
 - ▶ Same targeting, different method



I'VE SEEN THIS BEFORE

- ▶ TTP similar to other botnets
 - ▶ Mirai, Kraken, Maris, ..
- ▶ Began with custom malware, ended with crimeware
- ▶ Used for DDoS and especially cover for operations

**IF IT TALKS LIKE A
CRIMINAL ..**

I'M A PROFESSIONAL. MY BUSINESS IS CRIME.

- ▶ It's not just botnets that look "cybercrime"
- ▶ "Ransomware" - destruction and / or cover
 - ▶ NotPetya, PartyTicket
- ▶ Crimeware, cybercrime infrastructure
 - ▶ Bulletproof-Hosting (e.g. Stark Industries)



**IT MIGHT BE A
CRIMINAL!**

OR AN ATTORNEY. OR BOTH. MEET "DJAMIX".

- ▶ A lot of cybercrime forums exist(ed)
 - ▶ Few attained the status of "Mazafaka"
- ▶ Launched in 2001, hacked in 2021
- ▶ "Djamix" was one of the most prolific members
 - ▶ Not a technical person, a lawyer
 - ▶ A .. special lawyer

[TLP:AMBER]

OR AN ATTORNEY. OR BOTH. MEET "DJAMIX".

- ▶ Brian Krebs dug into this alias after the hack
- ▶ "Djamix" aka Aleksei Safronov



OR AN ATTORNEY. OR BOTH. MEET "DJAMIX".

- ▶ Brian Krebs dug into this alias after the hack
- ▶ "Djamix" aka Aleksei Safronov
- ▶ Interesting "lawyer"
- ▶ But: No proof.
 - ▶ That batch is 10\$ online



THERE'S A PATTERN

- ▶ Multiple cybercrime actors work at "research institutes"
 - ▶ 46th Central Research Institute, MoD Center for Special Studies
 - ▶ Khamovnichesky Barracks
- ▶ TL;DR: They are GRU offices

THERE'S A PATTERN

- ▶ Multiple cybercrime actors work at "research institutes"
 - ▶ 46th Central Research Institute, MoD Center for Special Studies
 - ▶ Khamovnichesky Barracks
- ▶ TL;DR: They are GRU offices



THERE'S A PATTERN

- ▶ Multiple cybercrime actors work at "research institutes"
 - ▶ 46th Central Research Institute, MoD Center for Special Studies
 - ▶ Khamovnichesky Barracks
- ▶ TL;DR: They are GRU offices



THERE'S A PATTERN

- ▶ Multiple cybercrime actors work at "research institutes"
 - ▶ 46th Central Research Institute, MoD Center for Special Studies
 - ▶ Khamovnichesky Barracks
- ▶ TL;DR: They are GRU offices



FSB – DADDY'S FAVORITE

- ▶ It's basically the KGB (→ MSB → MB → FSK → FSB)
 - ▶ Except for FSO and SVR
- ▶ Principal Security Service
 - ▶ Putin: "Make FSB Great Again"
- ▶ Ton of tasks, ton of power, ton of reach



FSB – DADDY'S FAVORITE

- ▶ Internal security is a good place!
 - ▶ Known Who-is-Who
 - ▶ Chances for patronage
 - ▶ Chances for profit



EVIL CORP - A FAMILY AFFAIR

- ▶ In operation for 10+ years (excl. previous affiliations)
 - ▶ Previously tight-knit group, some with blood-ties
 - ▶ Still active today, although diminished
- ▶ Extorted more than 300 million USD from victims
 - ▶ Banking trojans, ransomware, ..
- ▶ \$5.000.000 bounty for the arrest of "Aqua"



EVIL CORP - A FAMILY AFFAIR

- ▶ In operation for 10+ years (excl. previous affiliations)
 - ▶ Previously tight-knit group, some with blood-ties
 - ▶ Still active today, although diminished
- ▶ Extorted more than 300 million USD from victims
 - ▶ Banking trojans, ransomware, ..
- ▶ \$5.000.000 bounty for the arrest of "Aqua"

EVIL CORP - THERE'S MORE FAMILY!

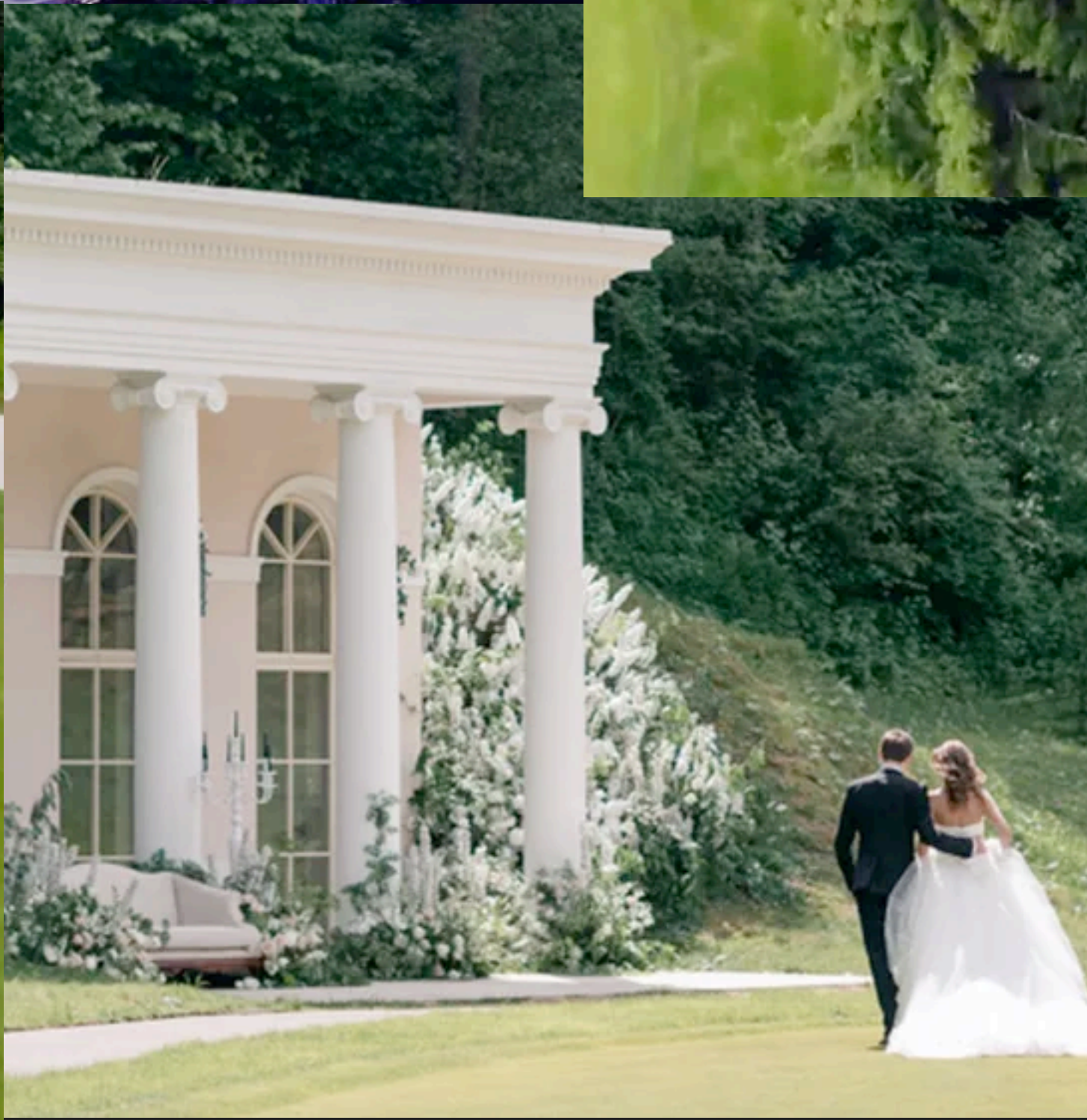
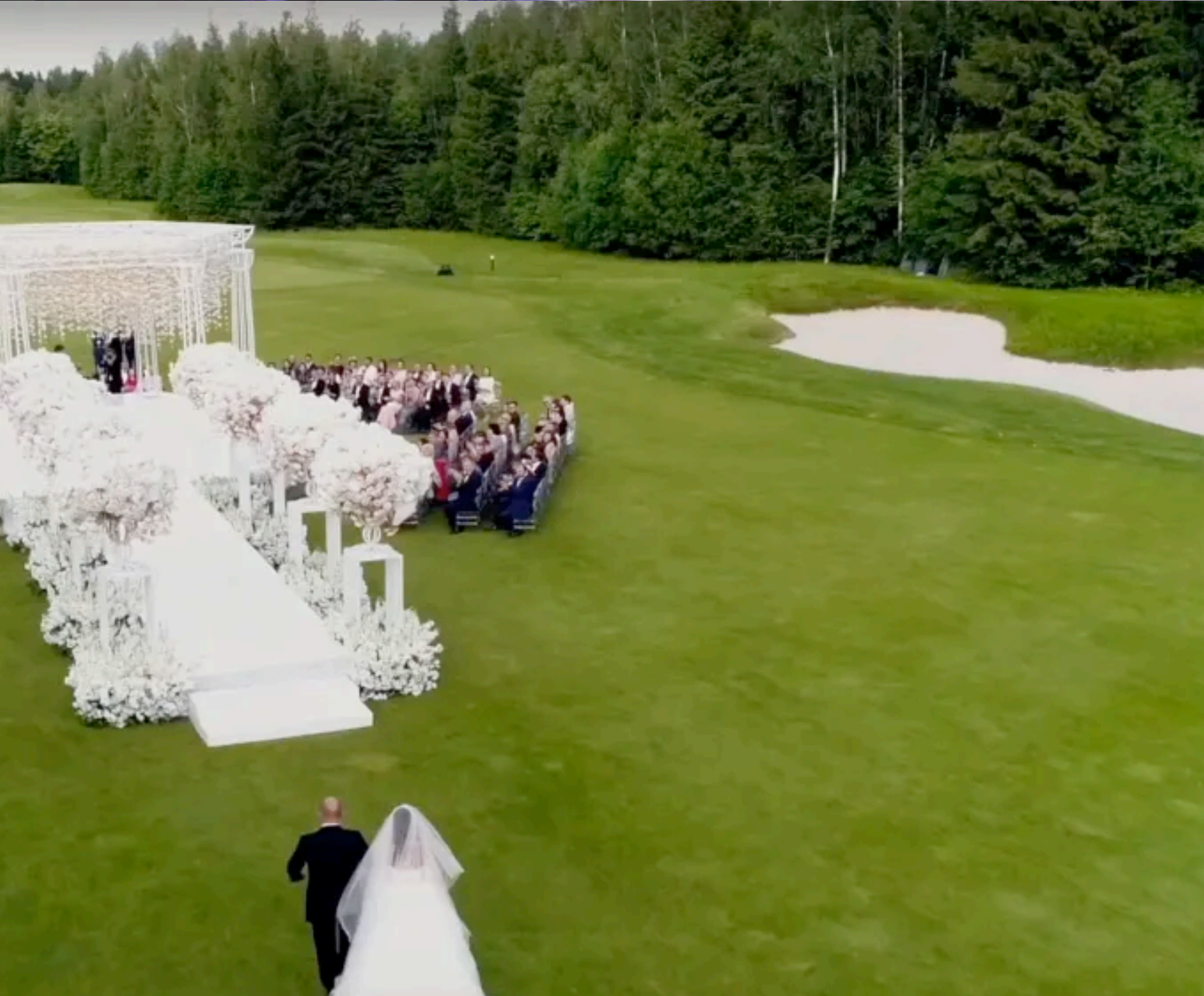
- ▶ Maksim Yakubets is an old hand
 - ▶ Jabber Zeus (2009), The Business Club (2011)
 - ▶ Dridex (~2011), Evil Corp (2014)
- ▶ Contacts to \$someone for a long while
 - ▶ Крыша is a necessity
 - ▶ Estimations: Since 2017



EVIL CORP - THERE'S MORE FAMILY!

- ▶ Maksim Yakubets is an old hand
 - ▶ Jabber Zeus (2009), The Business Club (2011)
 - ▶ Dridex (~2011), Evil Corp (2014)
- ▶ Contacts to \$someone for a long while
 - ▶ Крыша is a necessity
 - ▶ Estimations: Since 2017





IT'S NOT THAT HE MARRIED - IT'S WHO HE MARRIED

- ▶ Even cybercriminals get married, no big deal
- ▶ No more social media!

IT'S NOT THAT HE MARRIED - IT'S WHO HE MARRIED

- ▶ Even cybercriminals get married, no big deal
- ▶ No more social media!



[TLP:AMBER]

IT'S NOT THAT HE MARRIED - IT'S WHO HE MARRIED



IT'S NOT THAT HE MARRIED - IT'S WHO HE MARRIED

- ▶ Eduard Bandersky
 - ▶ "Former" member of KGB and Vympel
 - ▶ PMC Private security & hunting



IT'S NOT THAT HE MARRIED - IT'S WHO HE MARRIED

- ▶ Eduard Bandersky
 - ▶ "Former" member of KGB and Vympel
 - ▶ PMC Private security & hunting
- ▶ Linked to murder of Zelimkhan Khangoshvili
 - ▶ .. much retired, wow



THE FAMILY'S IN TROUBLE!

- ▶ Another feature of the Russian state: infighting
- ▶ FSB Division K is / was looking into Evil Corp
 - ▶ Stole money, tried to legalize it .. great target!
- ▶ But: GRU (might) have entered the building
 - ▶ Another member has blood-ties in that direction



[TLP:AMBER]



"THE FIGHT AGAINST CYBERCRIME IS THAT MATTER REGARDING WHICH RUSSIA HAS REPEATEDLY OFFERED COOPERATION."

- DMITRY PESKOV, PRESS SECRETARY FOR PUTIN



"THE FIGHT AGAINST CYBER THREATS IS A MATTER
REGARDING WHICH RUSSIA HAS REPEATEDLY OFFERED
COOPERATION."

- DMITRY PAVLOV, PRESS SECRETARY FOR PUTIN

THERE IS .. SO MUCH MORE.

- ▶ Sandworm (GRU) using Dark Crystal Rat, Rhadamantys Stealer, ..
- ▶ DaVinci Group and .. probably the FSB
- ▶ FSB and the Yahoo Hackers
- ▶ REvil and Fluffy / Emma Hill .. and probably \$someone
- ▶ ..

TO SUMMARIZE

- ▶ Russian cybercrime is part of the “hybrid state”, as most criminals are
- ▶ Russian intelligence services are aware of cybercrime & opportunities
 - ▶ Cybercrime can enable intelligence agencies
- ▶ Don't ignore stealers and other “basic stuff”
- ▶ International cooperation with Russia is (mostly) impossible
 - ▶ Yeah, arrests do happen. But those are interest-driven

TELL ME MORE, БЛЯДЬ!

- ▶ [World Cybercrime Index](#) by Dr. Miranda Bruce and Dr. Jonathan Lusthaus
- ▶ INSIKT (Recorded Future) does great work
- ▶ Works by Mark Galeotti, Danzig Baldaev, Solschenizyn, ..
- ▶ "[Хакер, Репа, Провив, Спы](#)" by Will Thomas
- ▶ "[The Cyber Vory](#)" by Gerry Johansson

THANK YOU FOR YOUR ATTENTION

- ▶ Comments, questions, recommendations, job offers*:
 - ▶ contact@bytesandborscht.com
- ▶ Social stuff:
 - ▶ bytesandborscht.com
 - ▶ @bytesandborscht (mostly screenshots from ebooks)

* I have no self-control, no other hobbies & no social life, but reasonable research skills and a bit of experience. Hire me!