MIDNIGHT
BLUE

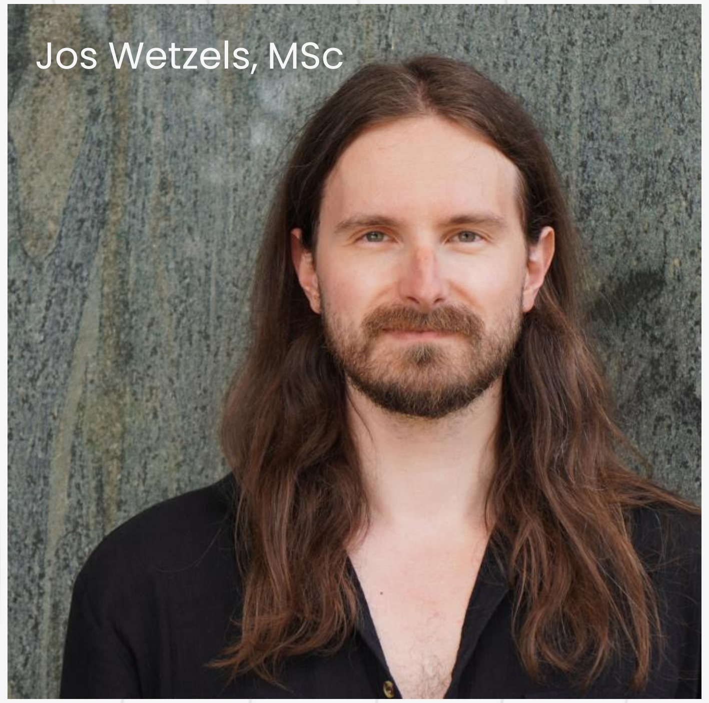
September 2024

ALL COPS ARE BROADCASTING

Breaking TETRA after decades in the shadows

By Midnight Blue

Midnight Blue


Jos Wetzels, MSc

Carlo Meijer, MSc

Wouter Bokslag, MSc

FCA PSA

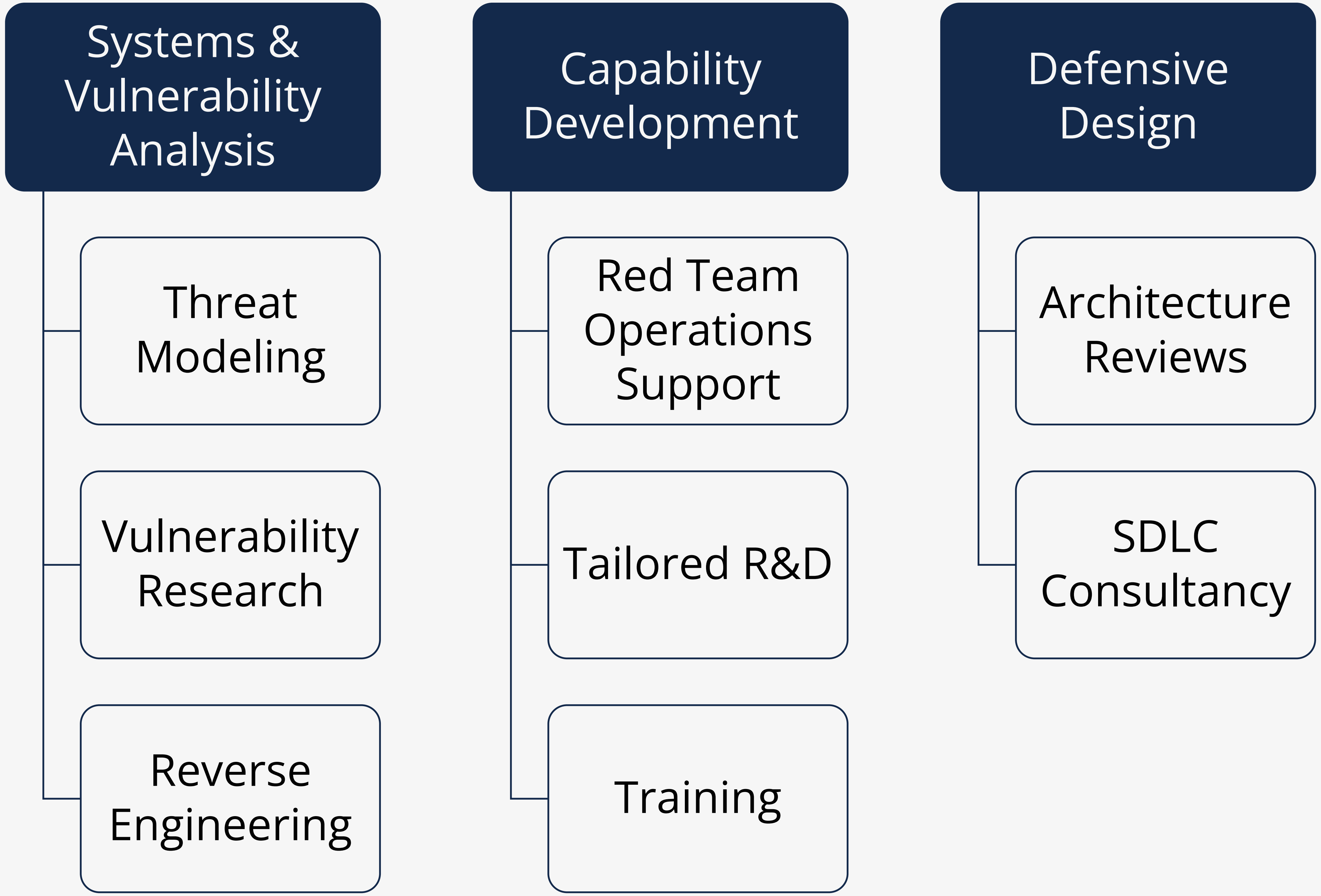
BlackBerry®

QNX®

MIFARE Classic

Selected Research

Services



Systems & Vulnerability Analysis

- Threat Modeling
- Vulnerability Research
- Reverse Engineering

Capability Development

- Red Team Operations Support
- Tailored R&D
- Training

Defensive Design

- Architecture Reviews
- SDLC Consultancy

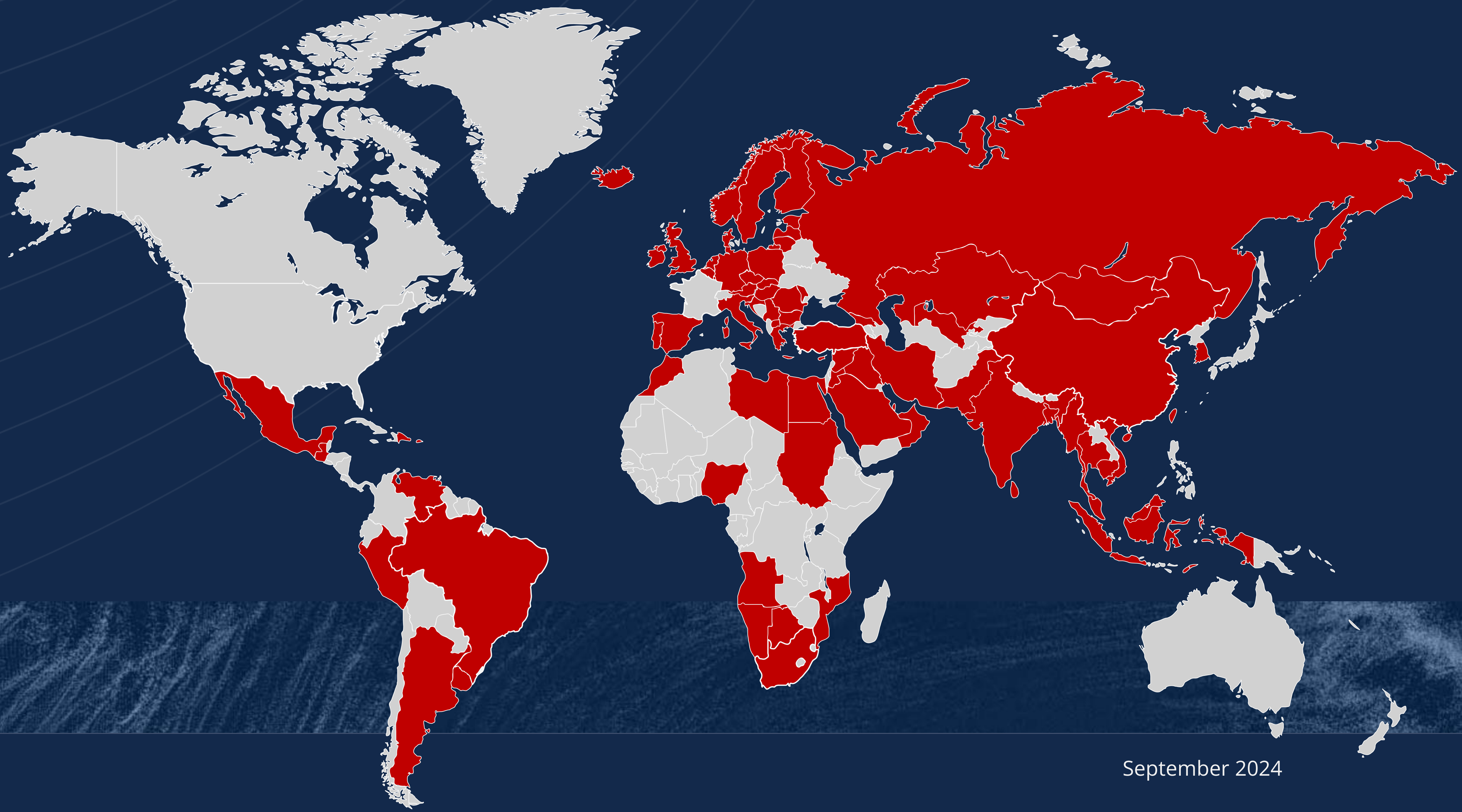
What is TETRA?

- Globally used radio technology
  - Competes with P25, DMR, TETRAPOL
- Standardized in 1995 by ETSI
  - Known for GSM, 3G/4G/5G, GMR, etc.
- Used for voice & data communications incl. machine-to-machine
- Relies on secret, proprietary cryptography

Use by police

Vast majority of global police forces use TETRA radio technology.

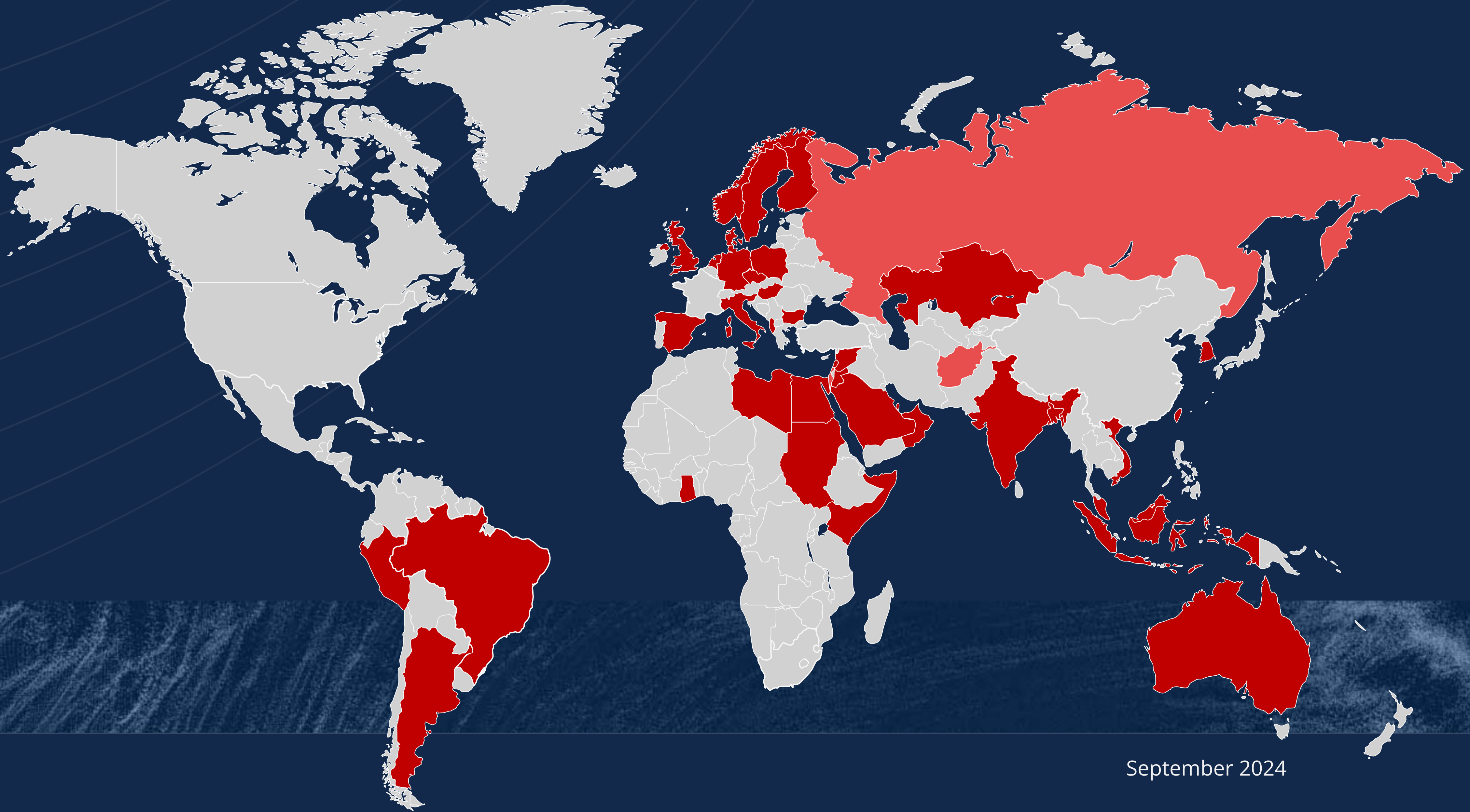
- C2000 (NL)
- ASTRID (BE)
- BOSNET (DE)
- AIRWAVE (UK)
- Nødnett (NO)
- Rakel (SE)
- SINE (DK)
- VIRVE (FI)
- SIRESP (PT)
- …



Based on OSINT

Military & Intelligence

Many countries have one or more military or intelligence units using TETRA radio technology as primary, fallback, or interfacing comms.

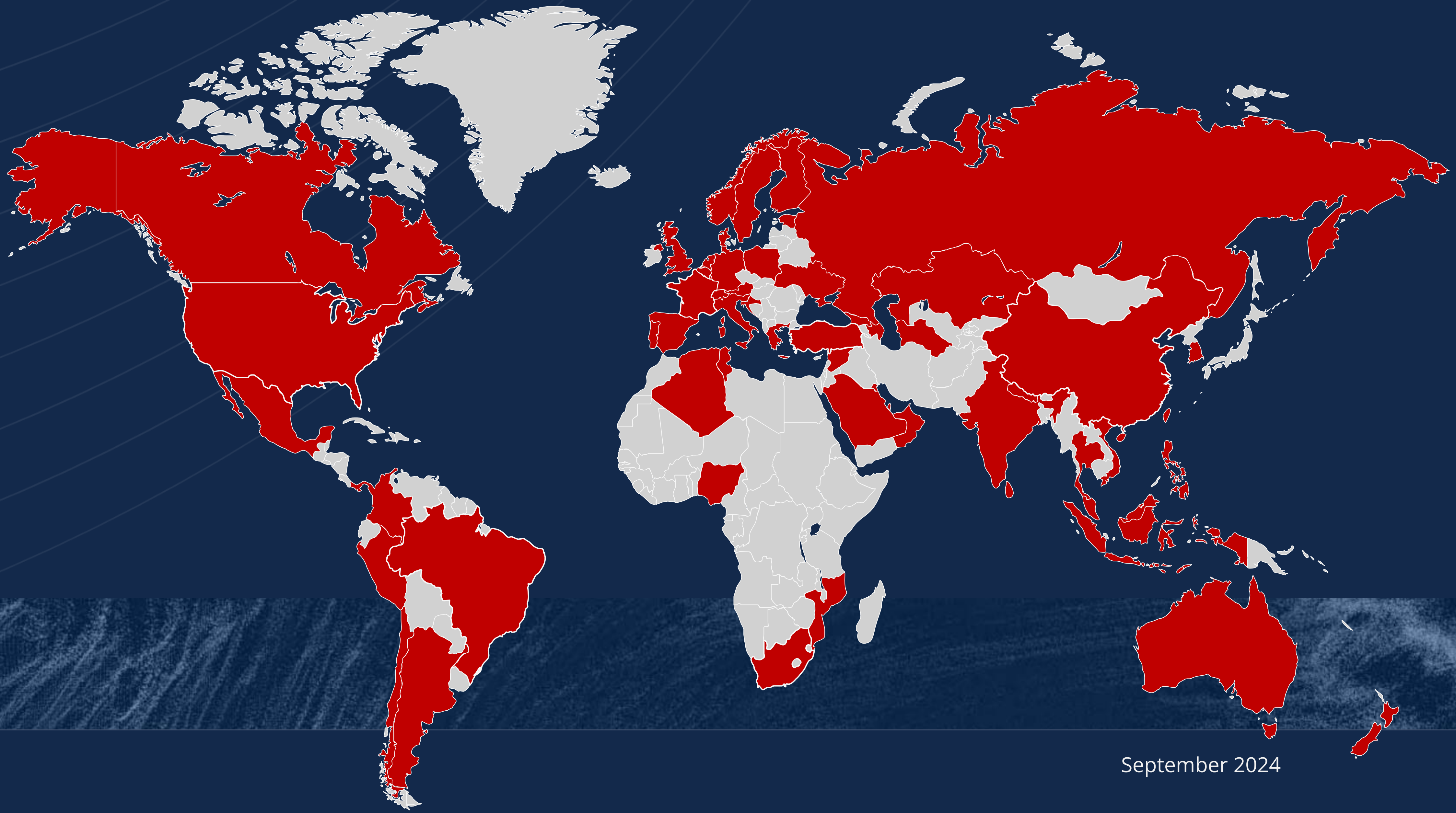


Based on OSINT

Critical Infrastructure

Many parties such as airports, harbors, and train stations use TETRA for voice communications.

In addition TETRA is used for SCADA WAN, such as substation & pipeline control, or railway signalling.

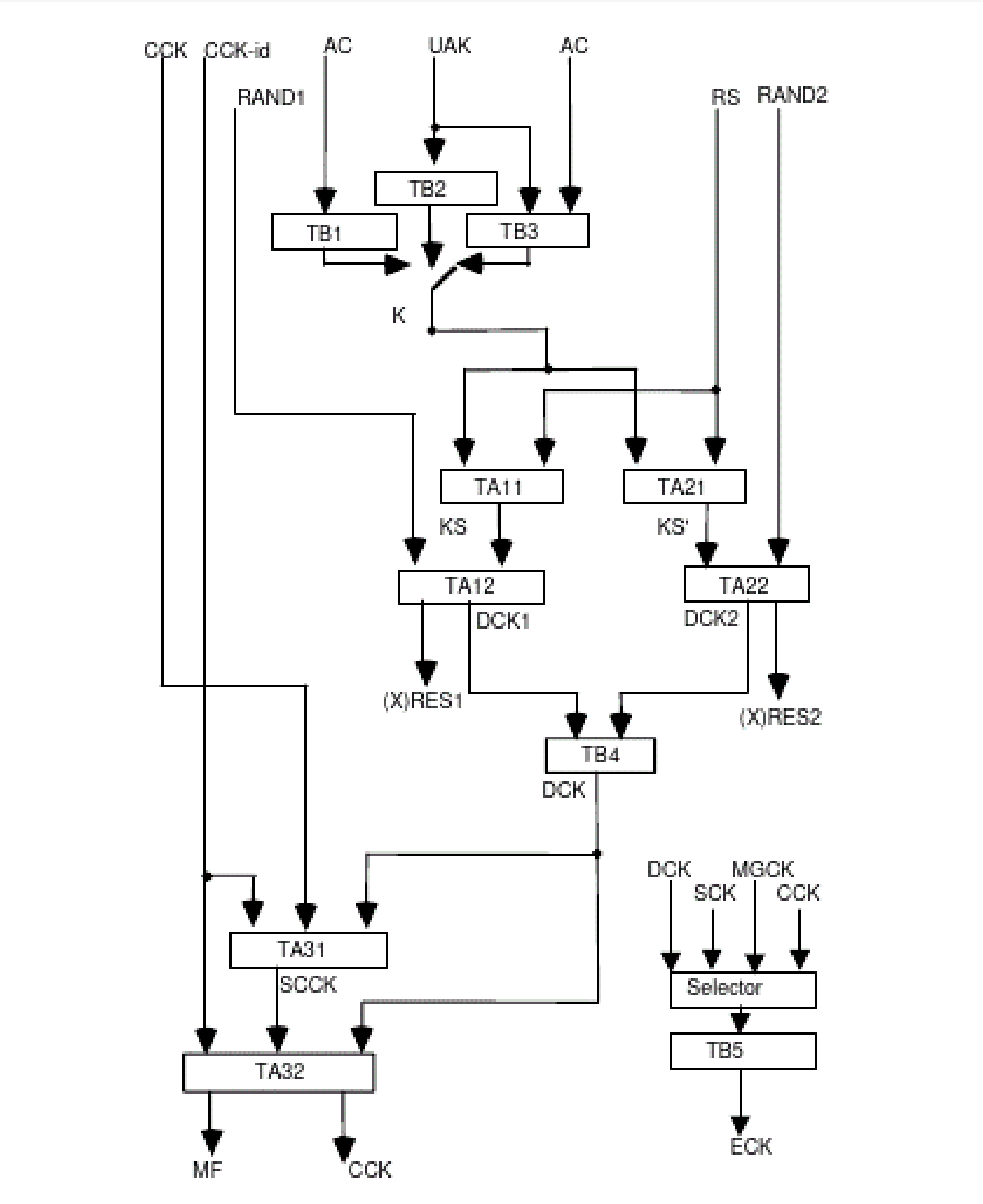


Based on OSINT

Open standard?

- Public standard, secret crypto
  - NDAs, only available for 'bona fide' parties

- Manufacturers must protect algorithms
  - Hardware, or, implementations
  - Software with extraction countermeasures



ure B.1: Overview of air interface authentication and key management (sheet 1

Lots of ‘bona fide’ vendors

Significant amount of geographically dispersed players

Top-tier adversaries likely have specs (e.g. via in-country manufacturers or theft)

Hytera
AIRBUS
sepura
LEONARDO
ROHILL
DAMM
FUNK-ELECTRONIC
piciorgros
GMBH
THALES
COBHAM
telm
энгстрем

Historical M&As

Teltronic, Simoco → Sepura, Nokia → Airbus, Rohde & Schwarz, PowerTrunk → Hytera, Selex ES → Leonardo, Chelton → Cobham, Artevea → dissolved.

TETRA security

- **TAA1 suite**
  - Authentication, key management / distribution (OTAR)
  - Identity encryption
  - Remote disable

- **TEA (TETRA Encryption Algorithm) suite**
  - Voice and data encryption (Air Interface Encryption (AIE))
    - **TEA1: Readily exportable**
    - **TEA2: European public safety**
    - **TEA3: Extra-European public safety**
    - **TEA4: Readily exportable (hardly used)**
  - Not to be confused with Tiny Encryption Algorithm!

Project RE:TETRA

Kerckhoffs’ principle

“A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.”

-Auguste Kerckhoffs, 1883

Violators don’t fare well

- A5/1, A5/2 (GSM), COMP128 (GSM)
- GMR-1, GMR-2 (SATPHONES)
- GEA-1, GEA-2 (GPRS)

- DSAA, DSC (DECT)
- MIFARE (RFID)
- HITAG (RFID)
- MEGAMOS (RFID)

- DST (RFID)
- Legic (RFID)
- CSS (DVD)
- CryptoAG / Hagelin

- Orange = backdoored

~~Kerckhoffs’ principle~~
ETSI’s principle

> **“Well [obscurity is] also a way of maintaining security.”***
>
> -Brian Murgatroyd, Chairman ETSI TC TETRA, 2023

* Interview between Kim Zetter and Brian Murgatroyd, Chair of ETSI TC TETRA
https://zetter.substack.com/p/interview-with-the-etsi-standards

Project motivation

- Proprietary cryptography has repeatedly suffered from practically exploitable flaws which remain unaddressed until disclosed

- GOAL: open up TETRA for public review after 20+ years
  - Enables informed risk analysis
  - Resolve issues
  - Level playing field

- Funded by NLnet
  - NPO funding open IT projects

nlnet FOUNDATION

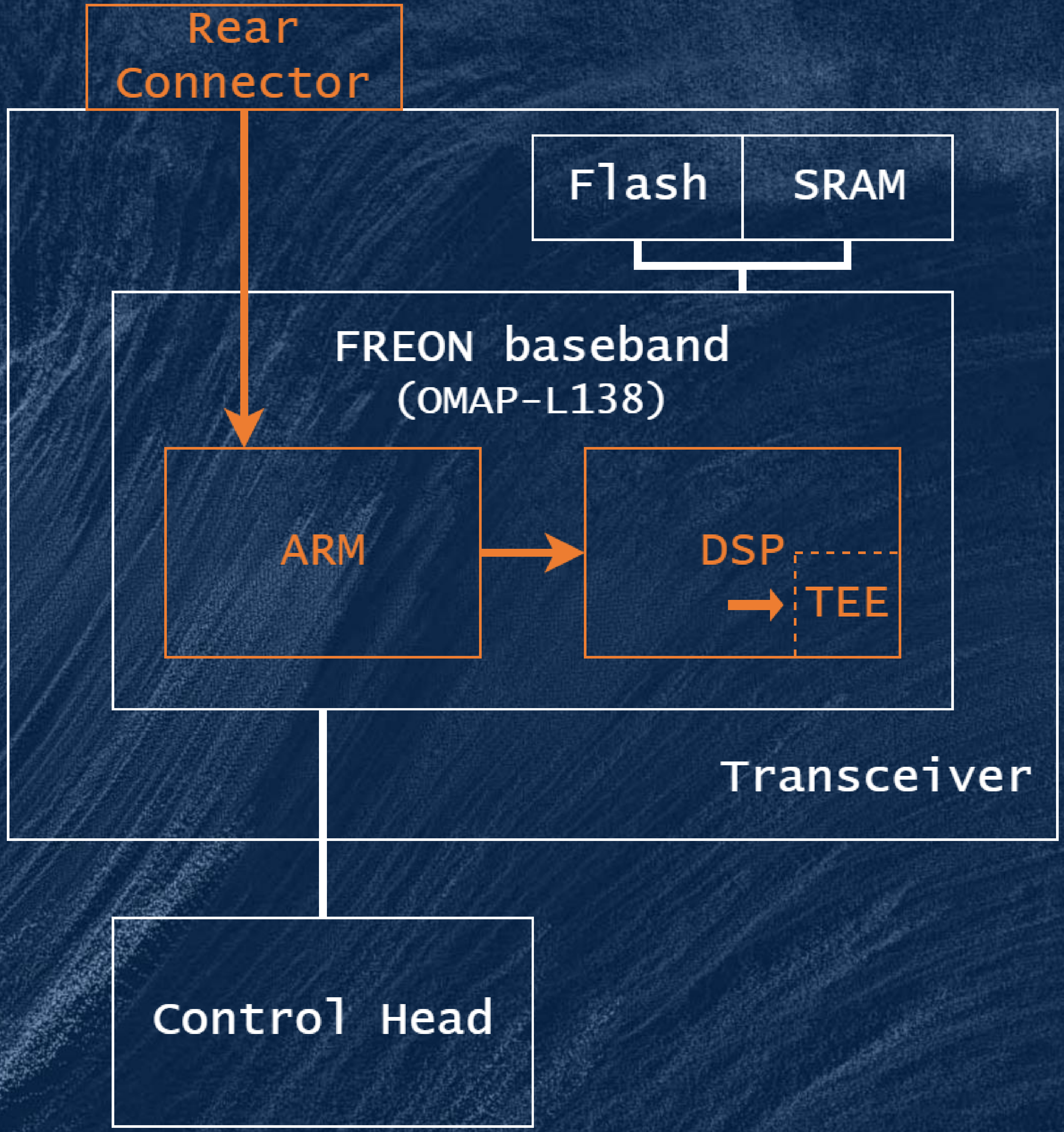
Let’s break open a radio!

Motorola MTM5400

- Common model, easily obtained 2nd hand online
- Baseband SoC by TI
  - So, no hardware TETRA crypto
- SoC has software security features
  - Used for protecting TETRA crypto from extraction?

Pwning MTM5400

1. Format string → code exec on AP
2. Pivot to DSP via shared memory
3. Cache timing side-channel on TEE
4. Secret algos!
   ... and key extraction ...
5. More details in our def con talk
   ... we only have 30 minutes here ☹



TETRABURST

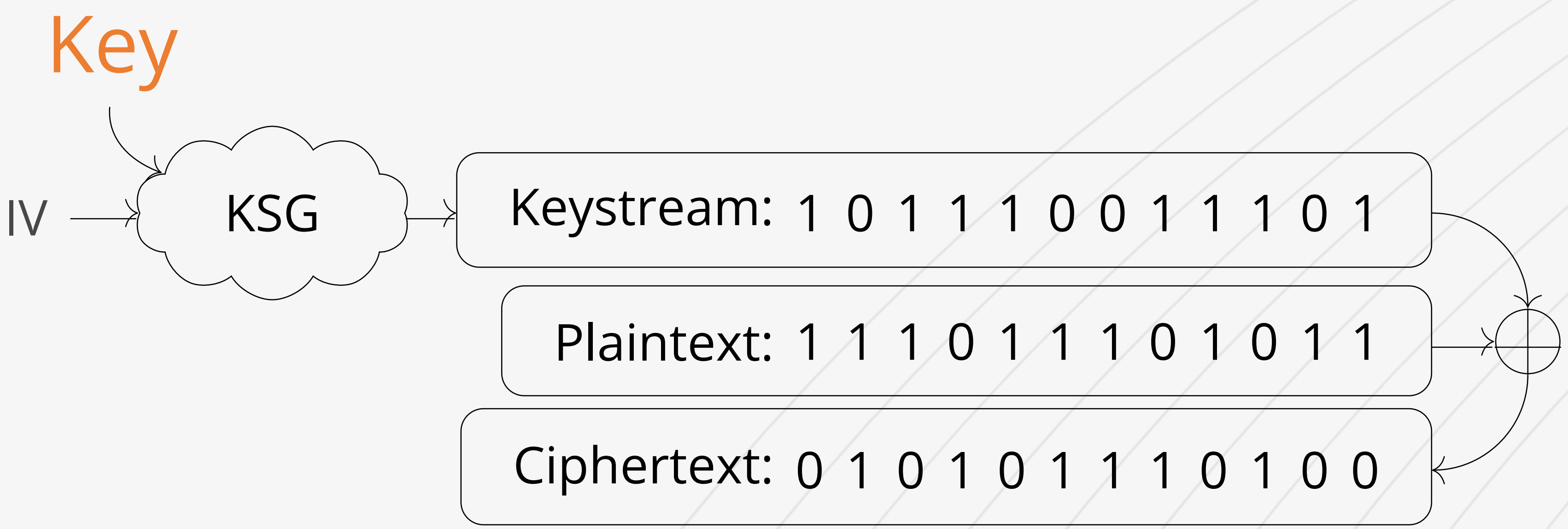
The secret TETRA primitives and their security

Stream cipher operation

- Key Stream Generator (KSG) generates keystream based on key*
  **and initialization vector*

- Encryption: combine plaintext with keystream using XOR

- Decryption: combine ciphertext with keystream again



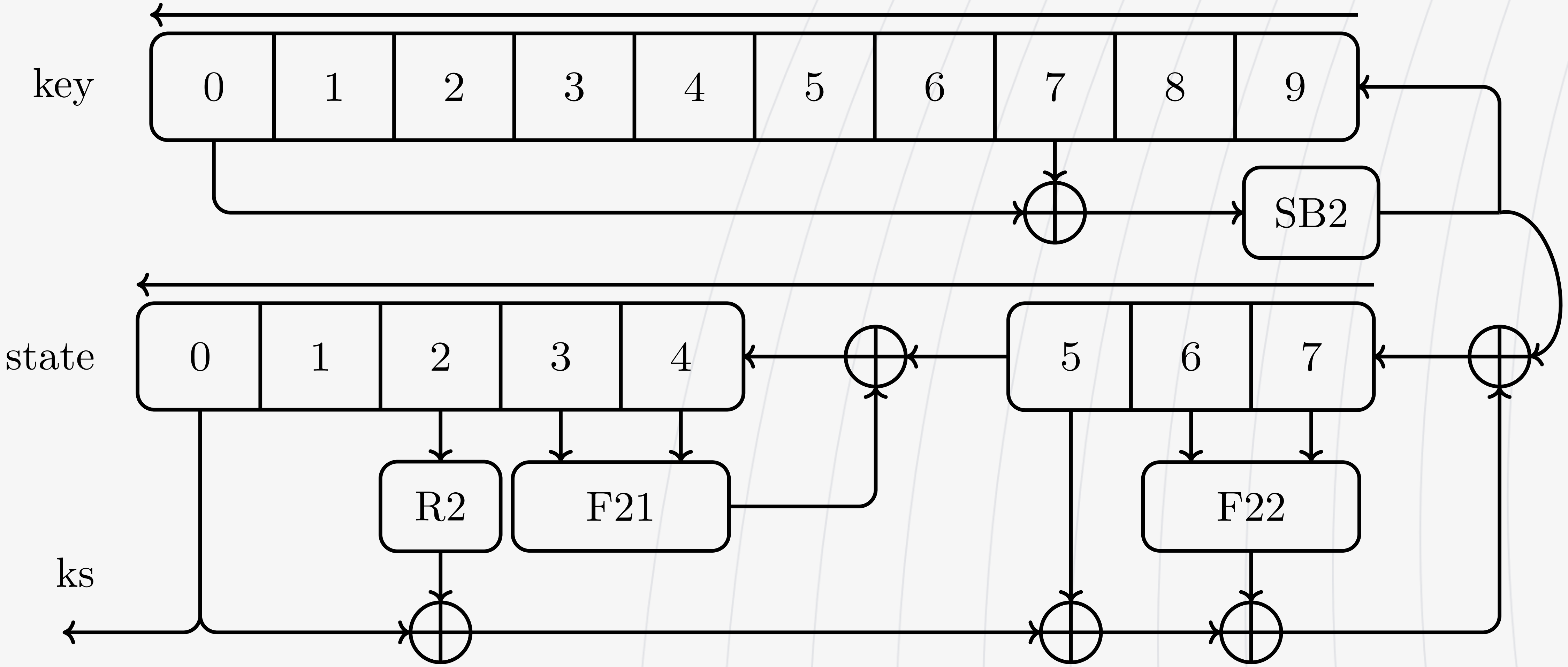
Keystream: 1 0 1 1 1 0 0 1 1 1 0 1

Plaintext: 1 1 1 0 1 1 1 0 1 0 1 1

Ciphertext: 0 1 0 1 0 1 1 1 0 1 0 0

TEA Keystream generators

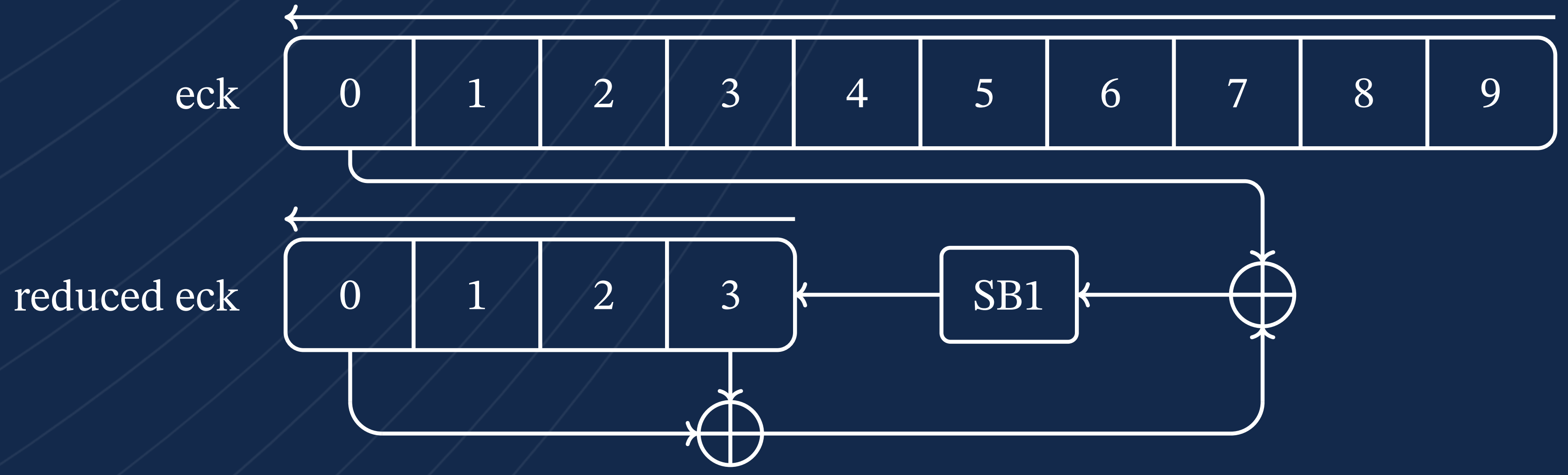
- Used for air interface encryption
- All KSGs have similar structure
- TEA2 seems robust*
  - We are not cryptographers
  - Public scrutiny needed!

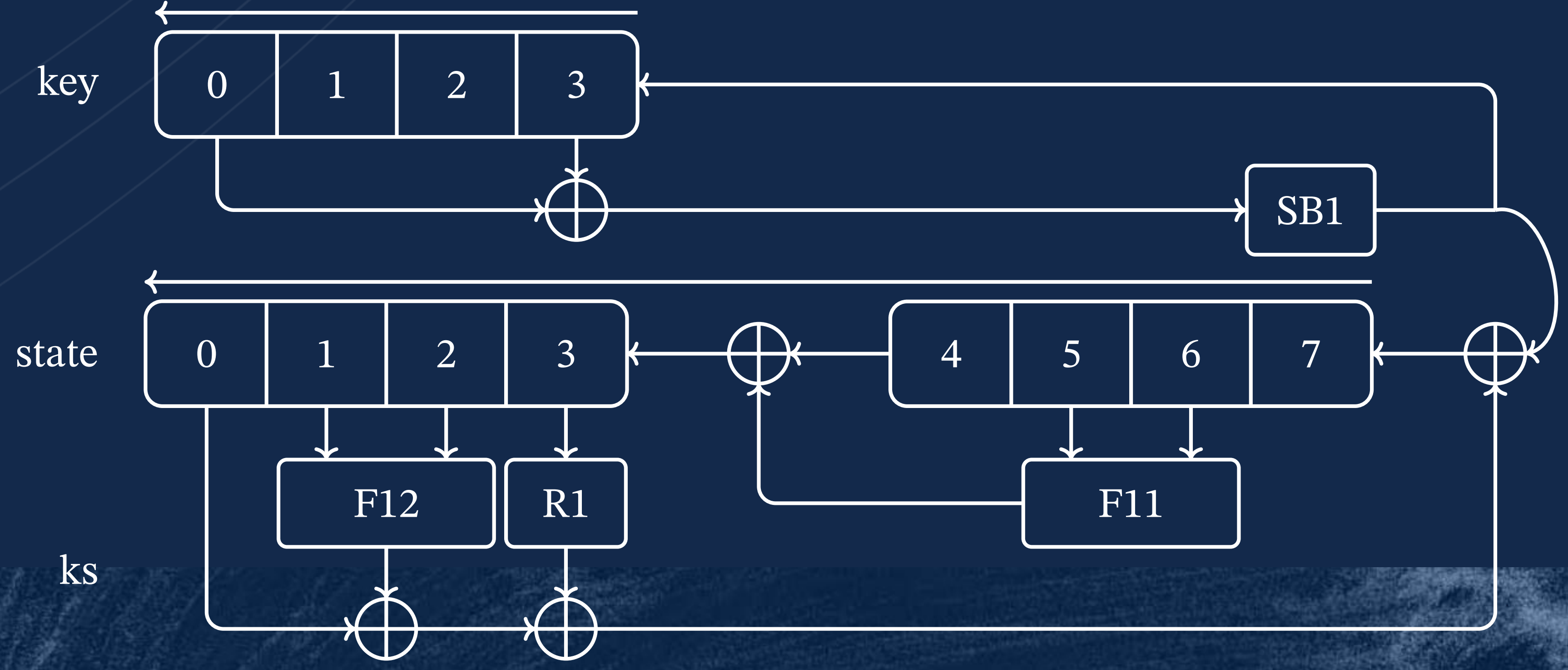


Pictured: TEA2

CVE-2022-24402
TEA1 backdoor

- Target audience
  - Private security, “less friendly” police / mil
  - .. But also, power, water, oil & gas
- Advertised with 80-bit key
  - Readily exportable but no hard indication on actual security (56-bit? 40-bit? 32-bit?)
- Has “key initialization” function
  - Reduces 80-bit key into 32-bit register
- Trivial passive brute force (<1min)
  - Intercept comms
  - Inject data (SCADA WAN!)





NVIDIA GTX 1080

State-of-the-art… consumer hardware… in 2016…

"**BM**: The researchers found that they were able to decrypt messages from this, using a **very high-powered graphics card** in about a minute."[1]

"**BM**: I suppose all I can say is that **25 years ago the length of this algorithm was probably sufficient to withstand brute-force attacks**.
KZ: You're saying 25 years ago 32 bit would have been secure?
BM: I think so. I can only assume."[1]

"**BM**: I would say it's vulnerable if you happen to be an expert and have some **pretty reasonable equipment**."[1]

[1] Interview between Kim Zetter and Brian Murgatroyd, Chair of ETSI TC TETRA https://zetter.substack.com/p/interview-with-the-etsi-standards

- Let’s not assume

- Let’s not assume

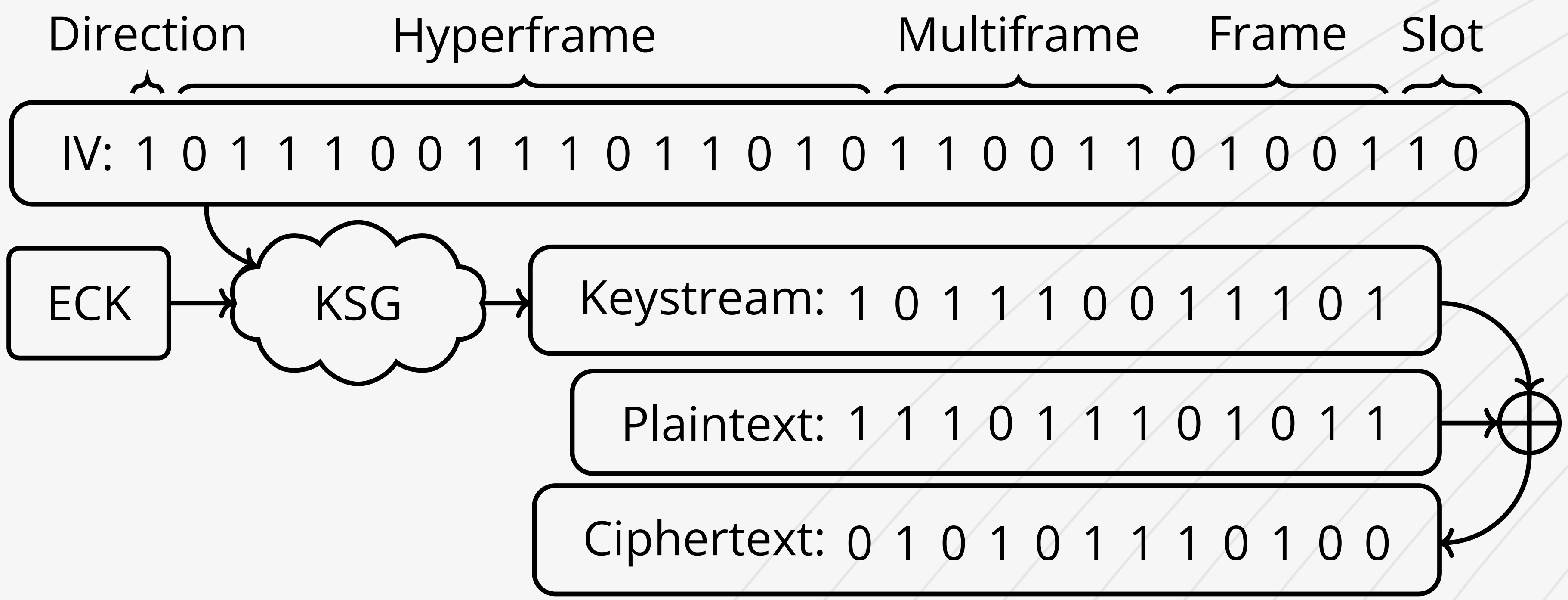
- Let’s not use reasonable equipment

Toshiba Satellite 4010CDS

- Let’s not assume
- Let’s not use reasonable equipment
- Let’s go back to 1998!
  - 266 MHz Pentium II
  - 4.1 billion byte hard disk
  - 32MB SDRAM

Demo: Party like the ‘90s

Air Interface Encryption


Direction
Hyperframe
Multiframe
Frame
Slot
IV: 1 0 1 1 1 0 0 1 1 1 0 1 1 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0
ECK
KSG
Keystream: 1 0 1 1 1 0 0 1 1 1 0 1
Plaintext: 1 1 1 0 1 1 1 0 1 0 1 1
Ciphertext: 0 1 0 1 0 1 1 1 0 1 0 0

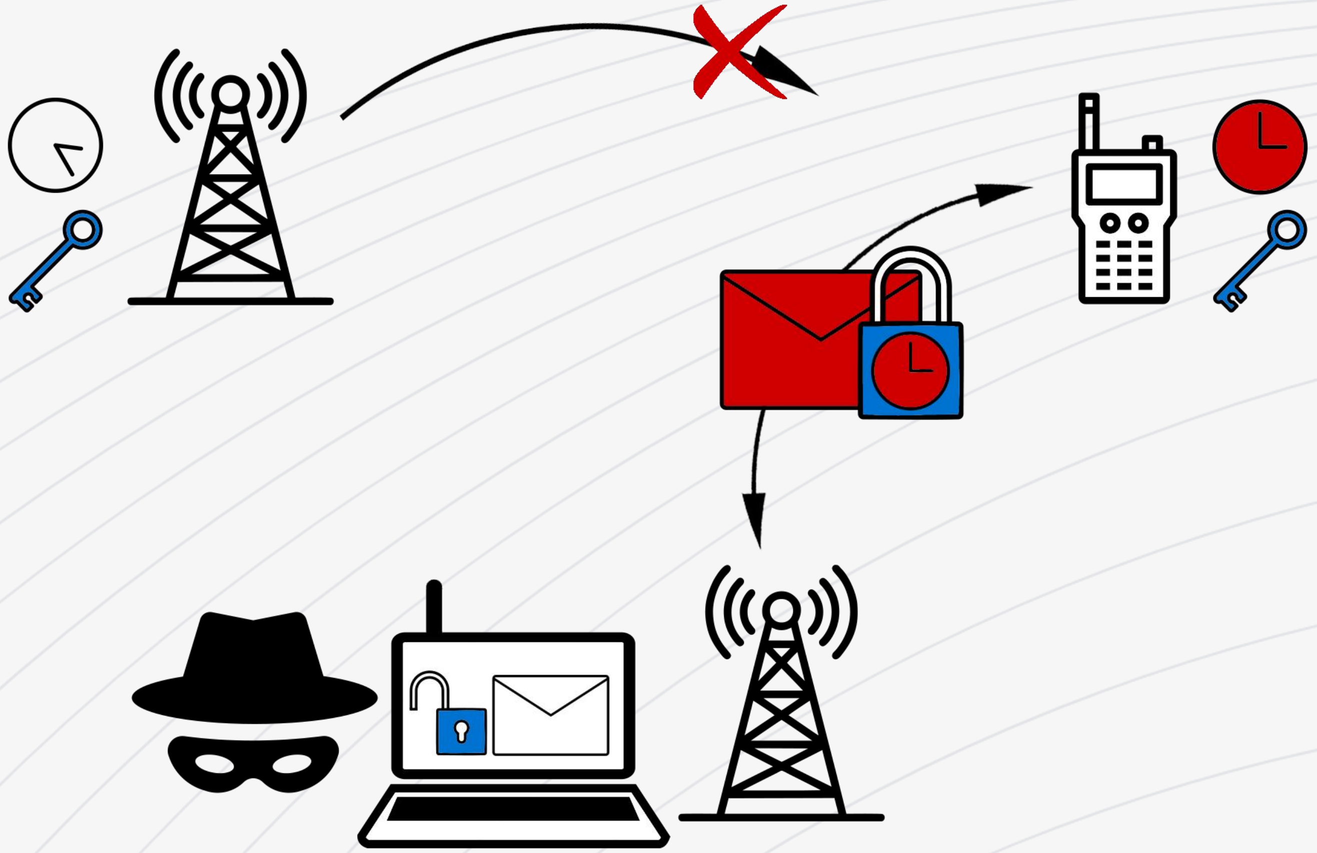
- **TEAx keystream generators depend on key and on network time**
  - Need to guarantee different keystream is used each time
- **Network time broadcast in unencrypted, unauthenticated manner**
  - SYNC and SYSINFO frames
- **Besides encryption, no further *cryptographic* integrity checks**
  - Any encrypted data is taken at face value

CVE-2022-24401 Keystream recovery attack

- Attacker can overpower infrastructure and alter MS perception of time
- MS will then use keystream that corresponds to the attacker-controlled network time
- Allows for re-use of keystream
- Works regardless of TEA used

Attack outline

- Capture interesting encrypted message at time T
- Target MS (any, with same keys)
- Overpower legitimate signal
- Set MS time to time T
- *Somehow recover keystream for that time*
- …
- Profit

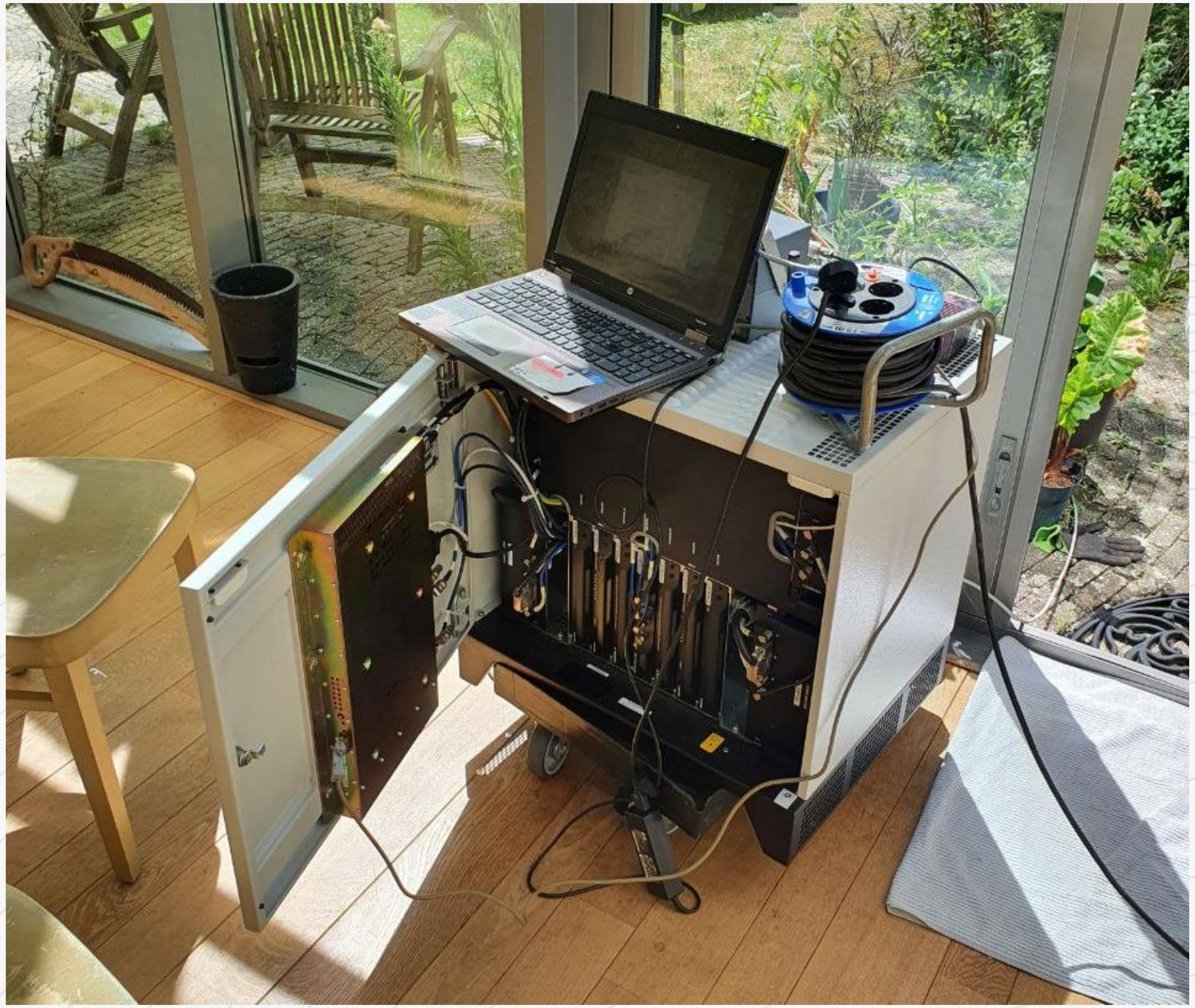


Intermezzo: ETSI

- “Theoretical attack”
- Okay, so, can we have a base station to prove practicality?
  - Haha lol no
  - More stakeholders responded like this
- What do we do now?
  - Implement TETRA infra stack for SDR?
  - Sounds like a lot of work…

There's your PoC

- Bought old Motorola MBTS
- Found some vulns in it
- Wrote module framework for it
- Turned it into attack platform 💪



Demo: CVE-2022-24401

Keystream recovery attack

Further issues

- **TETRA:**
  - De-anonymization attack
  - Session key pinning attack
- **Texas Instruments OMAP-L138**
  - 3 CVEs in ROM code
  - Breaking Secure Boot and TEE
- **Motorola**
  - 4 CVEs on MTM5x00 radio firmware
  - 5 CVEs on EBTS base station firmware
  - Both allow for key extraction and persistent covert implants

Hold on ....

Surely the TEA1 backdoor doesn't impact Europe right?

Nobody would shoot themselves in the foot like that?!

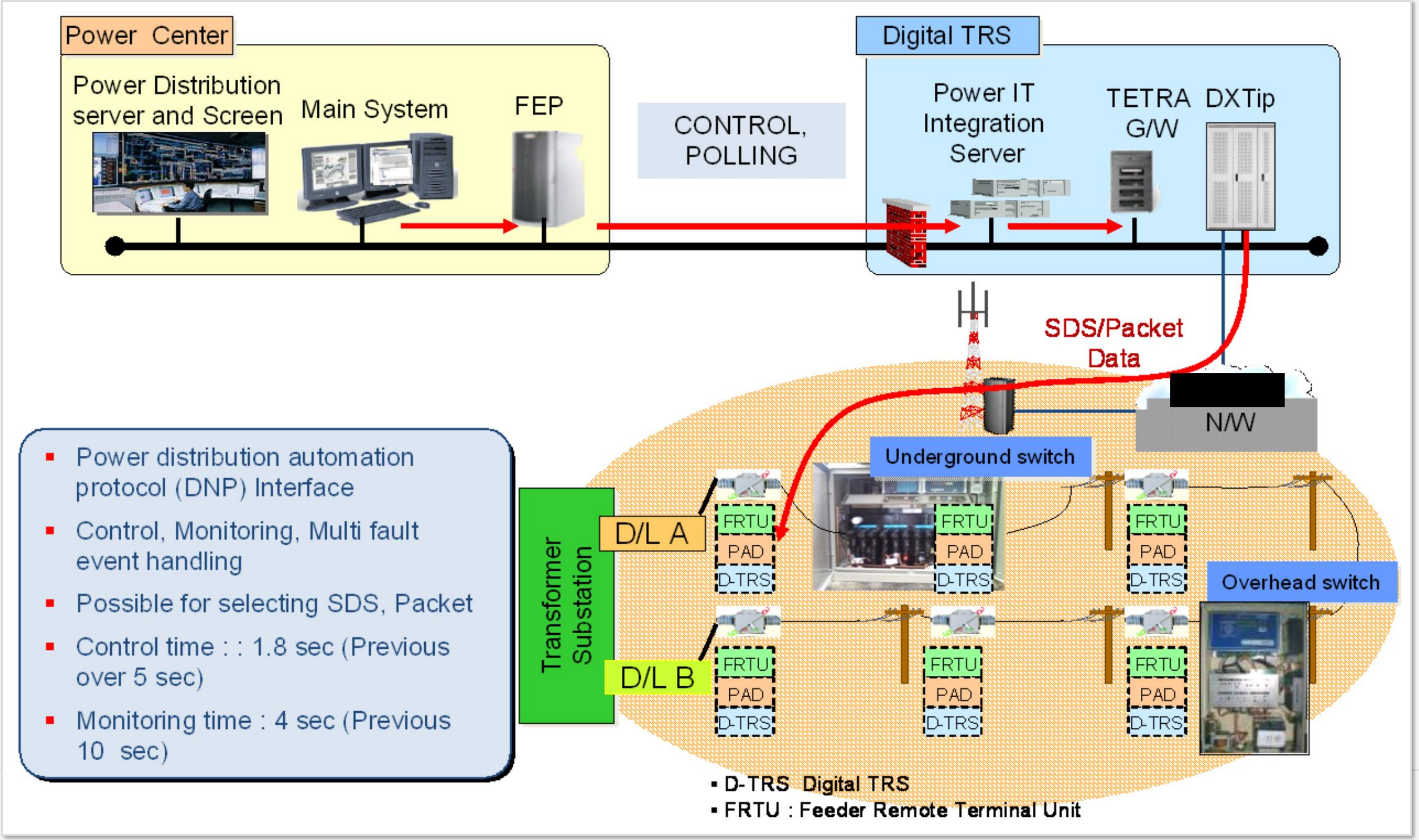
"**BM:** And I would expect that anybody ... who need a lot of protection would not just be using TEA1. Within Europe... I would suggest that anyone who needed high security would be using TEA2. .... The problems generally are that TEA2 is only licensed for use within Europe by public safety authorities."[1]

[1] Interview between Kim Zetter and Brian Murgatroyd, Chair of ETSI TC TETRA https://zetter.substack.com/p/interview-with-the-etsi-standards

TEA1 in Critical Infrastructure

- **HV, MV control in**
  - Germany
  - Poland
  - Luxembourg
  - Portugal
  - South Korea
  - Hong Kong
  - Georgia
  - South Africa
  - …

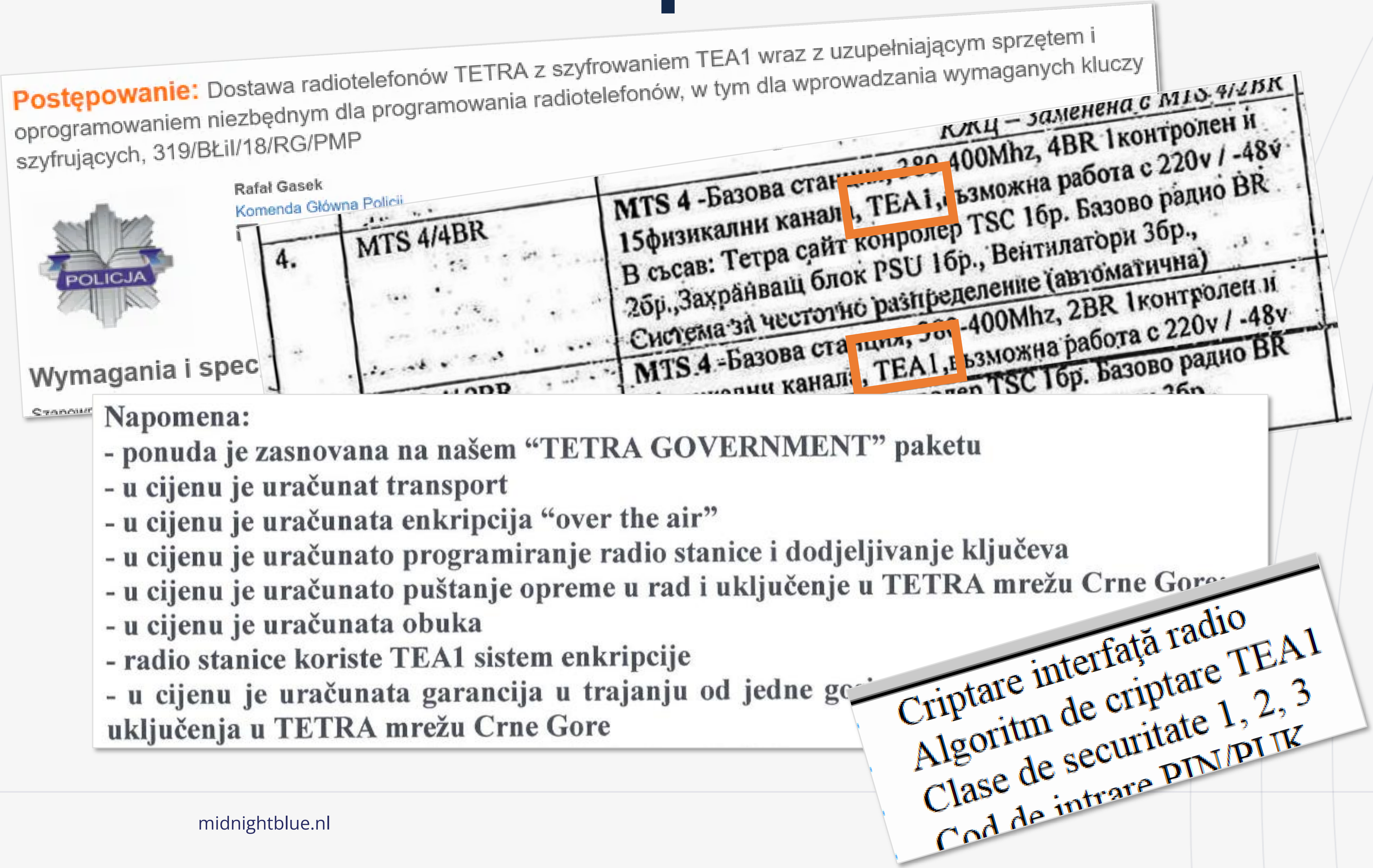
- **O&G control in**
  - Turkey
  - India
  - Saudi Arabia
  - Australia
  - Algeria
  - Nigeria
  - Peru
  - …



- Power distribution automation protocol (DNP) Interface
- Control, Monitoring, Multi fault event handling
- Possible for selecting SDS, Packet
- Control time : : 1.8 sec (Previous over 5 sec)
- Monitoring time : 4 sec (Previous 10 sec)

- D-TRS Digital TRS
- FRTU : Feeder Remote Terminal Unit

“Not a problem”



Postępowanie: Dostawa radiotelefonów TETRA z szyfrowaniem TEA1 wraz z uzupełniającym sprzętem i oprogramowaniem niezbędnym dla programowania radiotelefonów, w tym dla wprowadzania wymaganych kluczy szyfrujących, 319/BŁiI/18/RG/PMP

Rafał Gasek
Komenda Główna Policji

Wymagania i spec

		КЖЦ – заменена с MTS 4/2BR
4.	MTS 4/4BR	MTS 4 -Базова стан[illegible], 380-400Mhz, 4BR 1контролен и 15физикални канал, TEA1, възможна работа с 220v / -48v В съсав: Тетра сайт конролер TSC 1бр. Базово радио BR 2бр.,Захранващ блок PSU 1бр., Вентилатори 3бр., Система за честотно разпределение (автоматична)
	[illegible]2BR	MTS 4 -Базова станция, 380-400Mhz, 2BR 1контролен и [illegible] канали, TEA1, възможна работа с 220v / -48v [illegible]лер TSC 1бр. Базово радио BR [illegible] 3бр.

Napomena:
- ponuda je zasnovana na našem “TETRA GOVERNMENT” paketu
- u cijenu je uračunat transport
- u cijenu je uračunata enkripcija “over the air”
- u cijenu je uračunato programiranje radio stanice i dodjeljivanje ključeva
- u cijenu je uračunato puštanje opreme u rad i uključenje u TETRA mrežu Crne Gore
- u cijenu je uračunata obuka
- radio stanice koriste TEA1 sistem enkripcije
- u cijenu je uračunata garancija u trajanju od jedne go[illegible] uključenja u TETRA mrežu Crne Gore

Criptare interfață radio
Algoritm de criptare TEA1
Clase de securitate 1, 2, 3
Cod de intrare PIN/PUK

TEA1 is not used in Europe, right?

- Poland: municipal police, 2020
- Bulgaria: defense, 2020
- Slovenia, aviation police, 2018
- Montenegro, police, 2018
- Moldova, police, 2020

Maybe nobody targets TETRA networks?

"**KZ:** But is that in the best interest of the public that are using these algorithms?

BM: Well it's a moot point isn't it, really. That's a difficult thing to say "yes it's to the benefit of the public or not." There's no evidence of any attacks on … TETRA that we know of."[1]

"ETSI and TCCA are not at this time aware of any exploitations on operational networks."[2]

2 out of 5 attacks are passive so… 🤔

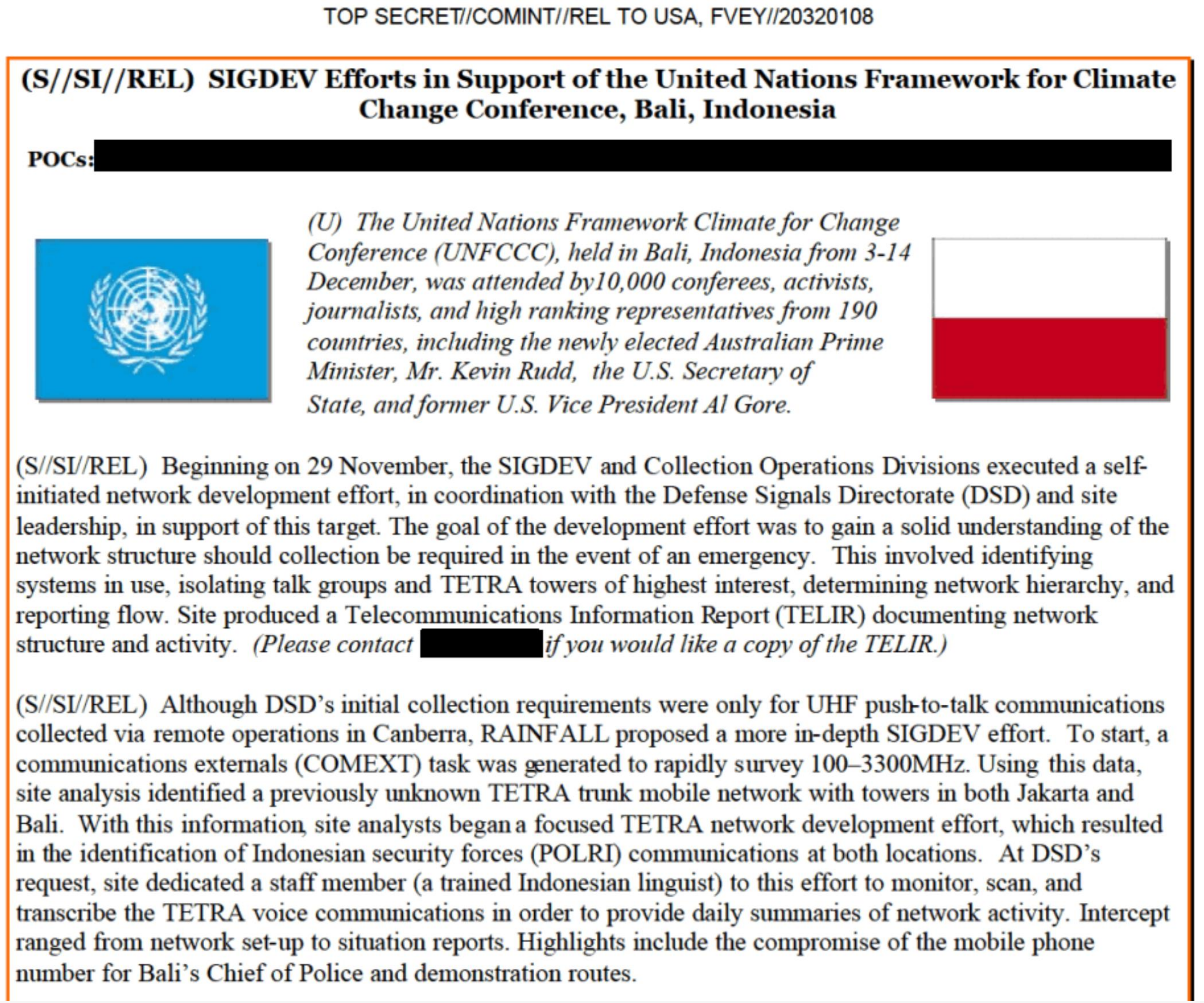
[1] Interview between Kim Zetter and Brian Murgatroyd, Chair of ETSI TC TETRA https://zetter.substack.com/p/interview-with-the-etsi-standards

[2] ETSI and TCCA Statement to TETRA Security Algorithms Research Findings Publication on 24 July 2023 https://www.etsi.org/newsroom/news/2260-etsi-and-tcca-statement-to-tetra-security-algorithms-research-findings-publication-on-24-july-2023

Right…

Snowden leaks show joint NSA & ASD project to collect Indonesian police TETRA comms during U.N. climate change conf in Bali 2007[1]

Not proof of TETRA:BURST exploitation specifically – but proof of *active TETRA targeting*



TOP SECRET//COMINT//REL TO USA, FVEY//20320108

(S//SI//REL) SIGDEV Efforts in Support of the United Nations Framework for Climate Change Conference, Bali, Indonesia

POCs: [redacted]

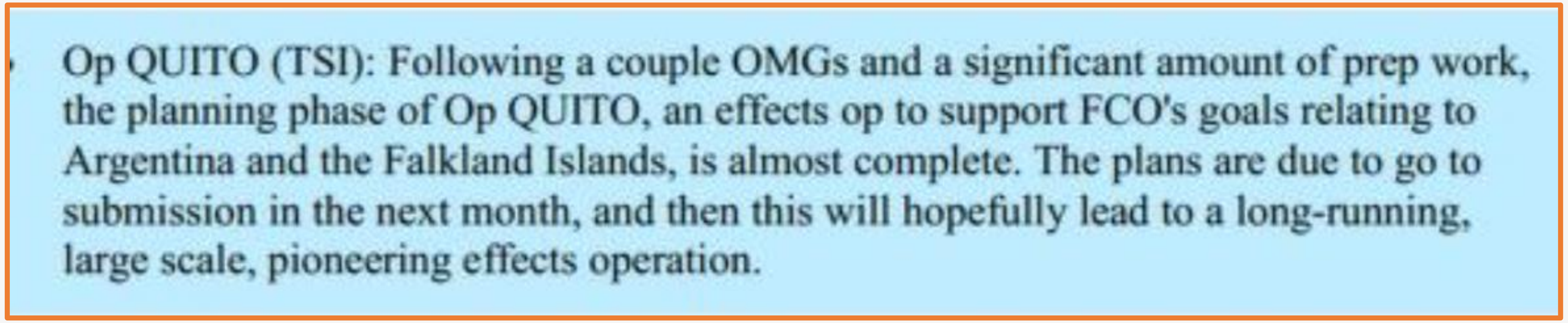
(U) The United Nations Framework Climate for Change Conference (UNFCCC), held in Bali, Indonesia from 3-14 December, was attended by10,000 conferees, activists, journalists, and high ranking representatives from 190 countries, including the newly elected Australian Prime Minister, Mr. Kevin Rudd, the U.S. Secretary of State, and former U.S. Vice President Al Gore.

(S//SI//REL) Beginning on 29 November, the SIGDEV and Collection Operations Divisions executed a self-initiated network development effort, in coordination with the Defense Signals Directorate (DSD) and site leadership, in support of this target. The goal of the development effort was to gain a solid understanding of the network structure should collection be required in the event of an emergency. This involved identifying systems in use, isolating talk groups and TETRA towers of highest interest, determining network hierarchy, and reporting flow. Site produced a Telecommunications Information Report (TELIR) documenting network structure and activity. *(Please contact* [redacted] *if you would like a copy of the TELIR.)*

(S//SI//REL) Although DSD's initial collection requirements were only for UHF push-to-talk communications collected via remote operations in Canberra, RAINFALL proposed a more in-depth SIGDEV effort. To start, a communications externals (COMEXT) task was generated to rapidly survey 100–3300MHz. Using this data, site analysis identified a previously unknown TETRA trunk mobile network with towers in both Jakarta and Bali. With this information, site analysts began a focused TETRA network development effort, which resulted in the identification of Indonesian security forces (POLRI) communications at both locations. At DSD's request, site dedicated a staff member (a trained Indonesian linguist) to this effort to monitor, scan, and transcribe the TETRA voice communications in order to provide daily summaries of network activity. Intercept ranged from network set-up to situation reports. Highlights include the compromise of the mobile phone number for Bali's Chief of Police and demonstration routes.

[1] https://theintercept.com/document/nsa-telegraph-sigdev-efforts-in-support-of-the-united-nations-framework-for-climate-change-conference-bali-indonesia/

Right…

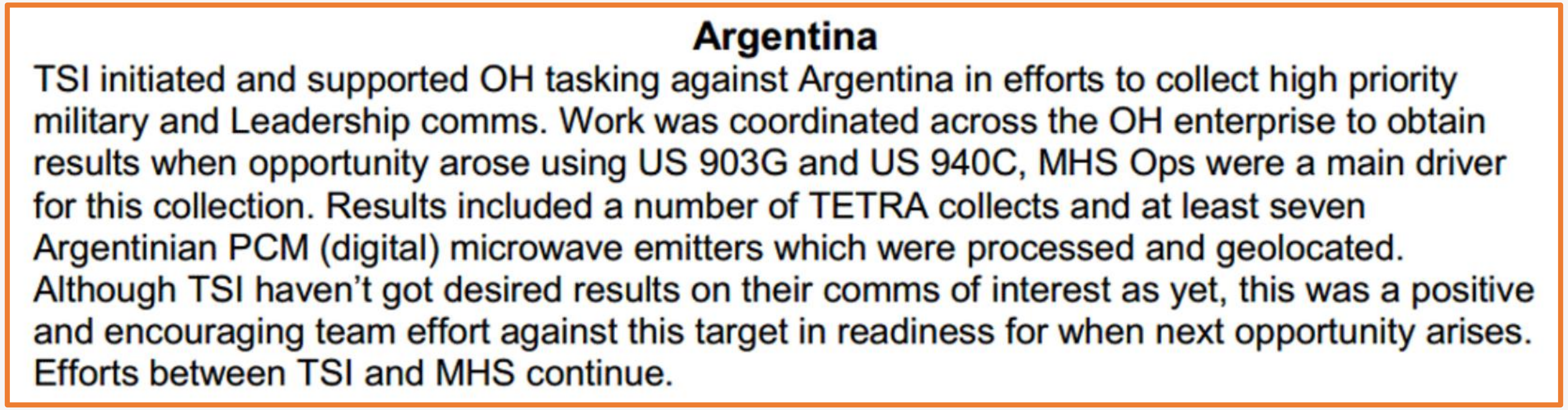


Op QUITO (TSI): Following a couple OMGs and a significant amount of prep work, the planning phase of Op QUITO, an effects op to support FCO's goals relating to Argentina and the Falkland Islands, is almost complete. The plans are due to go to submission in the next month, and then this will hopefully lead to a long-running, large scale, pioneering effects operation.

Snowden leaks reveal GCHQ TSI ‘*effects operation*’ QUITO against AR around Falklands/Malvinas oil exploration rights tensions in 2009[1]

Involved TETRA collects as part of military/leadership tasking

Not proof of TETRA:BURST exploitation specifically – but proof of *active TETRA targeting*



Argentina

TSI initiated and supported OH tasking against Argentina in efforts to collect high priority military and Leadership comms. Work was coordinated across the OH enterprise to obtain results when opportunity arose using US 903G and US 940C, MHS Ops were a main driver for this collection. Results included a number of TETRA collects and at least seven Argentinian PCM (digital) microwave emitters which were processed and geolocated. Although TSI haven't got desired results on their comms of interest as yet, this was a positive and encouraging team effort against this target in readiness for when next opportunity arises. Efforts between TSI and MHS continue.

[1] https://cryptome.org/2015/04/nsa-gchq-jtrig-intercept-15-0402.pdf

What’s next? New algos!

The new algorithms

- **Algorithm set B**
  - TAA2 authentication suite
  - TEA5-7 air interface encryption ciphers
- **Initially were to be secret but..**
- **Following our disclosures, old & new algos will be public!**

"Transparency is at the root of ETSI, in our governance and technical work. With their decision at the TCCE meeting, our members proved once again that we evolve with technology and market requirements," - Luis Jorge Romero, ETSI Director-General.

https://www.etsi.org/newsroom/press-releases/2293-etsi-releases-tetra-algorithms-to-public-domain-maintaining-the-highest-security-for-its-critical-communication-standard

Yay*

- **Assuming no sleight of hand**
  - Open design criteria
  - No unexplained constants
  - Open reference implementations
  - No rigging of manuals[1]

- **There's a clear front door now**

> *"The new algorithm TEA7 has an effective key length reduction to 56 bits and will be available in many countries as per the Wassenaar Arrangement."*

[1] https://www.cryptomuseum.com/intel/nsa/backdoor.htm#manual

[2] https://tcca.info/tetra/tetra-documentation/research_disclosures/

> *“Insanity is doing the same thing over and over again and expecting different results”*

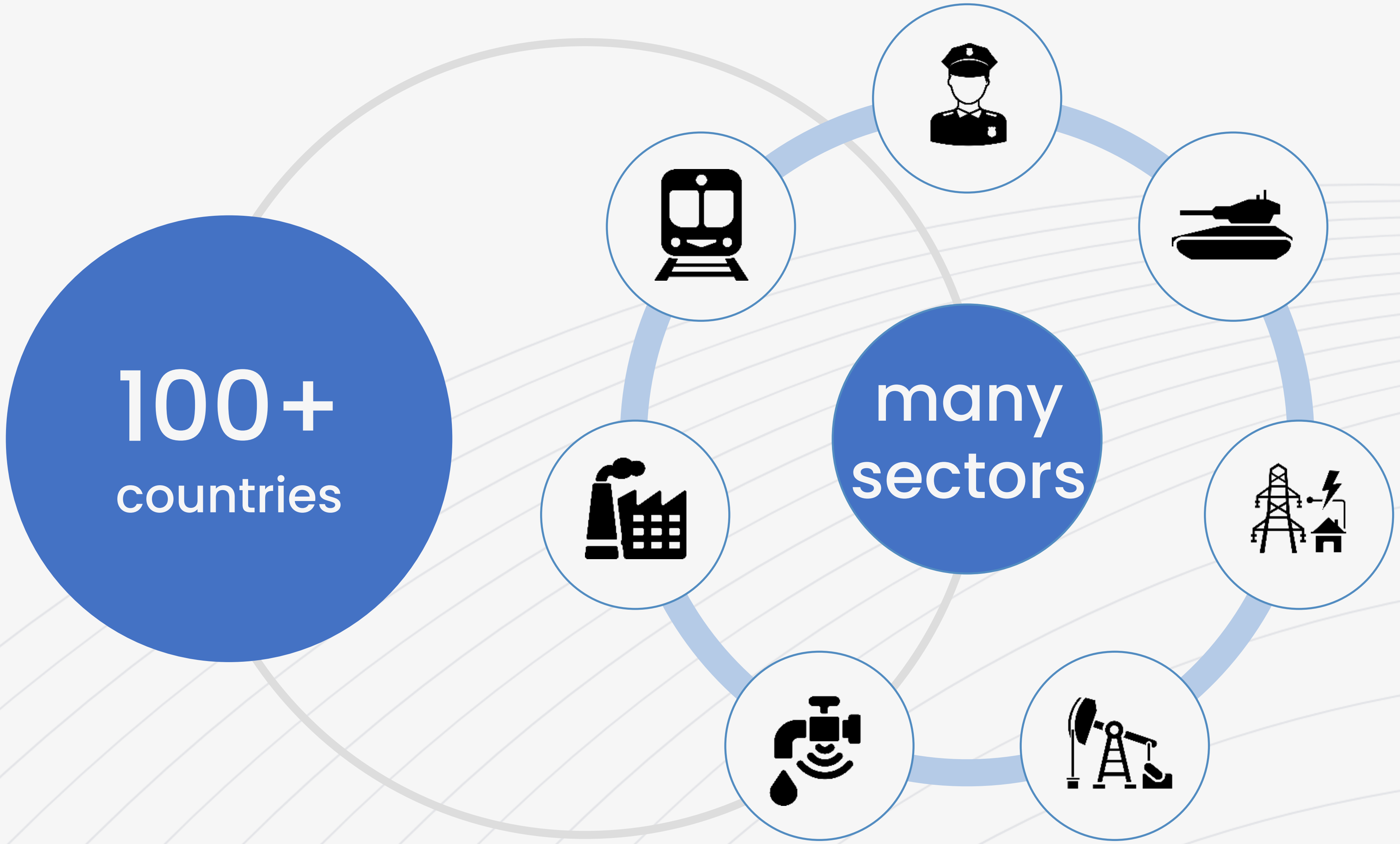
- **Wassenaar since year 2000:**
  - Exceptions for public crypto
  - Exceptions for (mobile) civil use
  - Exceptions for *“connected civil industry application“..*

- **Will critical infra get TEA7?**
  - As was the case for TEA1..
  - **This would be a big mistake**

- **At least now we know before adoption..**

Conclusion

- First public, in-depth TETRA security analysis (after 20+ years)
- Secret crypto algorithms reverse-engineered
- Multiple vulns found (incl. backdoor)
- Patches available for some issues, mitigations for others
- Lots of work still to be done for asset owners!



Questions?

MIDNIGHT BLUE

nlnet FOUNDATION

NGI ZERO PET

Social

- X in

Web

- midnightblue.nl
- tetraburst.com

Contact

- w.bokslag@midnightblue.nl