Phone Phreaking

telekomy chcą o tym zapomnieć

Warszawa, 2019-11-21

WYKORZYSTANE MATERIAŁY

- YouTube:
  - https://www.youtube.com/watch?v=4tHyZdtXULw
    Kanał: 8-bit Guy
    Wideo: How Telephone Phreaking Worked

  - https://www.youtube.com/watch?v=FufYSx2_6Bg
    Kanał: RCW39RJ
    Wideo: Hackers – The History of Hacking

  - Artykuły prasowe i strony internetowe
  - Doświadczenia własne 8^)

ETYMOLOGIA, CHRONOLOGIA I PRZYCZYNA

- Phone Phreaking
  - Słowo jest zlepkiem słów „*phone freak*".
  - Środowisko występowania: USA
  - Lata występowania: lata 60-te i 70-te
  - Przyczyny zaistnienia:
    - Wysokie koszty połączeń międzystrefowych
      - Przykład Davida Murraya (8-bit Guy): połączenie z Dallas (214) do Forth Worth (obszar 817) było traktowane jako zamiejscowe (naliczanie minutowe) mimo, że miasta są de facto obok siebie
      - Monopol Bell Systems skutkował cenami rozmów międzymiastowych w latach 60-tych na poziomie $5 za minutę, co obecnie przekłada się na ponad $35!
      - W Polsce było to mniej uciążliwe, np. cały Okręg Górnośląski miał kod 32 (032), Trójmiasto i okolice (włączając w to np. Hel) 58 (058) – podział na 49 województw*
    - Chęć poznania i „złamania" systemu
      - Pierwsi tzw. Gray Hats
      - To robin nasi dziadkowie!!!

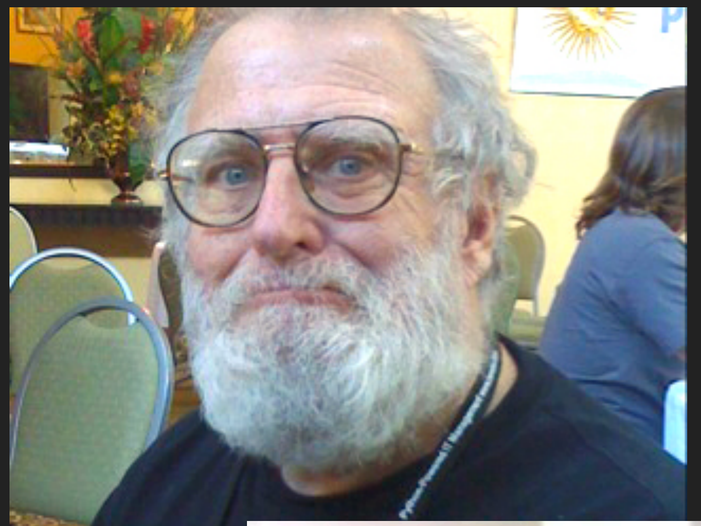
CAPTAIN CRUNCH

- Człowiek
  - John T. Draper
    „Captain Crunch“

- Rzecz
  - Płatki Cap’n Crunch
    - (1963-)
    - Dodawali „gratisy“
    - 2600 Hz po zakryciu jednej dziurki...

NIE TYLKO CAPTAIN CRUNCH...

- Ludzie
  - John T. Draper (1943-) aka „Captain Crunch”
    - W **Armii USA** od 1964
    - W jednostce pomagał wykonywać **darmowe połączenia telefoniczne** z
    - wojskowej centralki
    - Założył **pirackie radio WKOS** podczas odbywania służby w stanie Maine
    - Po służbie pracował nad pierwszymi **prototypami telefonów**
    - **bezprzewodowych** w National Semiconductors
    - Prowadził **audycje w radio KKUP w Cupertino, CA**
  - Dennis Terry (1954-) aka „Denny”
    - Jest osobą **ociemniałą**
    - Członek grupy ociemniałych **proto-phreakerów**
    - To on przekazał Draperowi infomację jak można wykorzystać **gwizdek dołączany**
    - **jako gratis do opakowania płatków** „Captain Crunch” – zadzwonił pod numer ogłaszany
    - przez Drapera podczas **testów pirackiego nadajnika radiowego** (sic!)
    - **https://youtu.be/FufYSx2_6Bg?t=280**
  - Josef Carl Engressia, Jr. (1949-) aka „Joybubbles”
    - Podobnie jak „Denny” jest osobą **ociemniałą** i należał do wsponianej **grupy ociemniałych proto-phreakerów**
    - Obiusly Denny nie umiał „gwizdać” dwóch tonów, ale centrale przyjmowały także **sygnalizację jednotonową SF** (impulsy)
    - Ma **perfekcyjny słuch**, to on zidentyfikował **częstotliwość 2600 Hz w gwizdku**



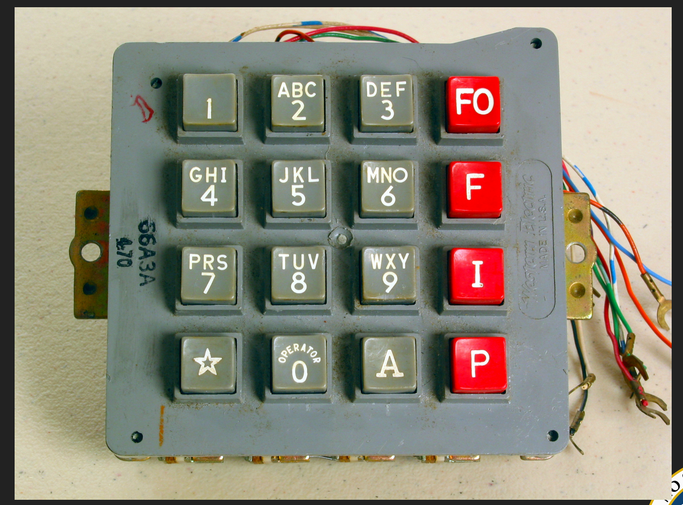
JAK TO DZIAŁAŁO? – DTMF

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

- Telefonia bardzo analogowa
- Wybieranie tonowe DTMF (Dial-tone Multi-frequency)
- Projekt: Bell System (1877-, teraz AT&T) w 1960
- Wdrożenie komercyjne: 18 Listopada 1963 (56 l.)
- Wciąż uzywany w radioamatorstwie a także do przekazywania caller ID (prócz FSK)
- Rozpoznawianie: zespoły filtrów w CA, obecnie algorytmem Goertzela, który dla ograniczonych zakresów częstotliwości jest prostszy w implementacji od FFT

  ciekawostka: Gerald Goertzel pracował przy projekcie Manhattan

- DTMF jest wciąż używany w radioamatorstwie a także do przekazywania caller ID (prócz FSK), no i Android Dialer!
- Nie zawiera tonu 2600 Hz!
- Dodatkowe klawisze A (FO) B (F) C (I) oraz D (P) mają specjalne znaczenie i są używane przez operatorów



JAK TO DZIAŁAŁO? – MAGICZNE 2600 HZ

- Centrale telefoniczne w tym czasie były najbardziej skomplikowanymi, cywilnymi systemami technicznymi używanymi publicznie w epoce przedinternetowej
- Wolne trakty międzycentralowe „gwizdały do siebie” tonem 2600 Hz
- Przykład tzw. „in-band signaling”

  W przeciwieństwie do „out-of-band signalling” czyli np. sygnalizacji SS7
- Sygnał 2600 Hz nie był filtrowany na pętli abonenckiej*
- Po jego wydaniu system oczekiwał nowego połączenia wybranego kodem MF, poprzednikiem DTMF, używanym wewnętrzne przez Bell Systems od lat 50-tych do sygnalizacji międzycentralowej
- Najprostrzy phreak call:
  - Zadzwoń na darmowy numer (w USA to numery 1-800)
  - Po pewnym czasie prześlij ton 2600 Hz (dla koneserów: E w 7. oktawie)
  - Wyślij ton KP (2t) cyfry (t) i ton ST (t) – (t) to czas trwania tonu i odstępu między tonami, zwykle 55 ms
  - Enjoy! 8^)

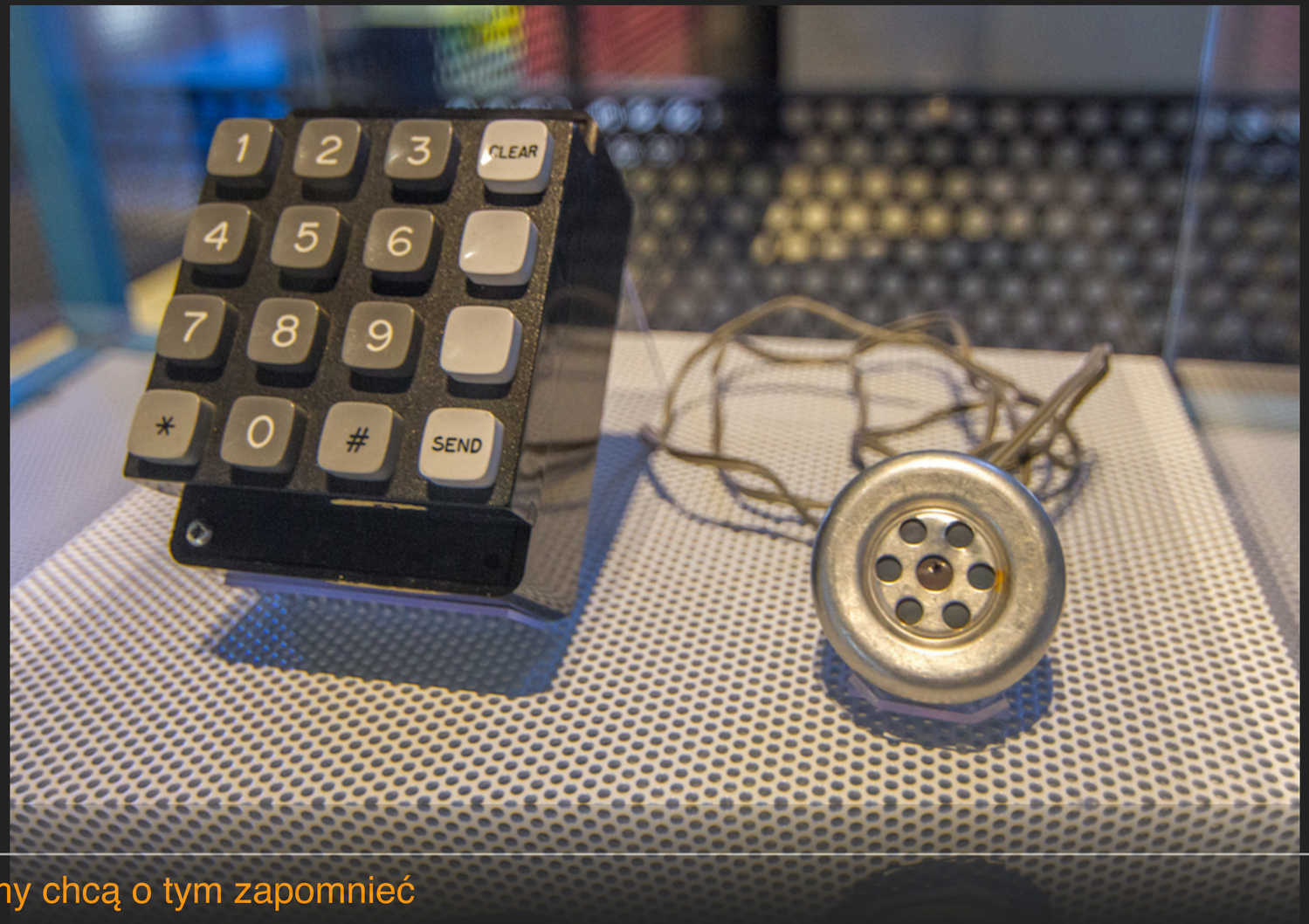
KP	1100	1700
KP2	1300	1700
Digit 1	700	900
Digit 2	700	1100
Digit 3	900	1100
Digit 4	700	1300
Digit 5	900	1300
Digit 6	1100	1300
Digit 7	700	1500
Digit 8	900	1500
Digit 9	1100	1500
Digit 0	1300	1500
ST	1500	1700

JAK TO DZIAŁAŁO? — BLUE BOX IS COMING

- Najprostrzy phreak call:
  - Zadzwoń na darmowy numer (w USA to numery 1-800)
  - Po pewnym czasie prześlij ton 2600 Hz (dla koneserów: E w 7. oktawie)
  - Wyślij ton KP (2t) cyfry (t) i ton ST (t) – t to czas trwania tonu i odstępu między tonami, zwykle 55 ms
  - Enjoy! 8^)
- Właśnie do tego grupa ociemniałych proto-phreakerów potrzebowała wiedzy Drapera – sami nie byli w stanie skonstuować urządzenia, które realizowałoby powyższe kroki
- Draper szybko to zrealizował nazywając urządzenie Blue Box od koloru obudowy projektowej, które kupił w sklepie z elektroniką…
- Filozoficzny przykład na to, że ograniczenia rodzą kreatywność.

JAK TO DZIAŁAŁO? – BLUE BOX

- Blue Box zbudowany przez Steve'a Woźniaka i używany przez niego i Steve'a Jobsa przed czasami Apple
- Eksponat w Computer History Museum w Mountain View, CA

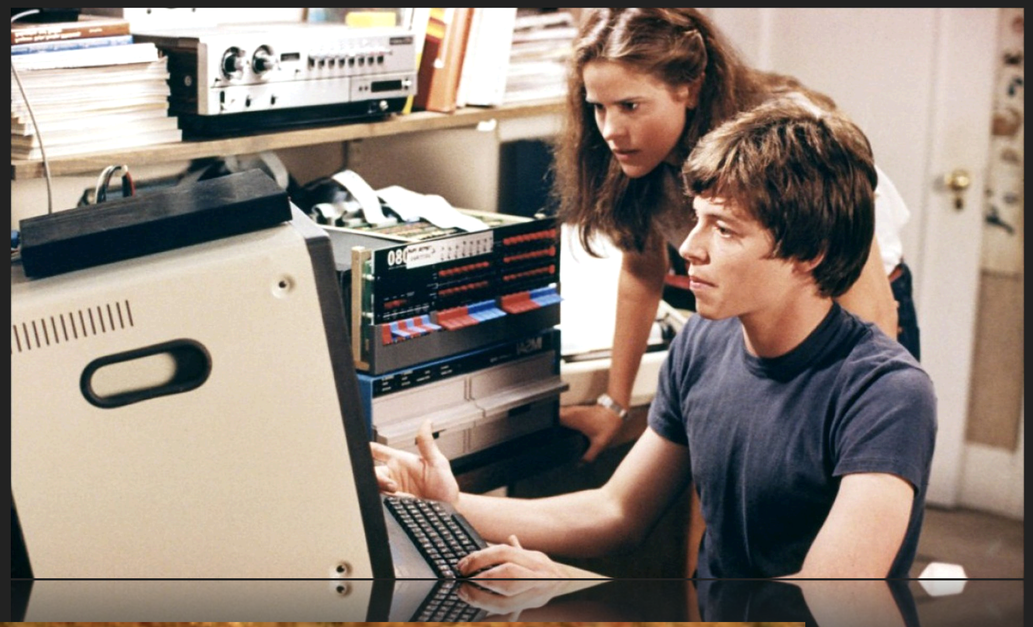


INNE BOKSY...

- Black Box – oszukiwał CA tak, aby nie zauważyła podniesienia słuchawki
- Red Box – emulacja tonów sygnalizacyjncyh telefonów publiczne (budek) – monety!
- Green Box – emulacja tonów telefonów publicznych (budek) – kody MF
- Beige Box – nie boks, ale określenie na wpinanie się do linii np. sąsiada…
- Clear Box – wzmacczniacz umożliwiający kontynuowanie rozmowy bez monet...
- Violet Box – rezystor, który działa jak Black Box – dla innego typu CA
- Gold Box – spinał dwie linie telefoniczne, by można było z drugiej zadzwonić
- **White** Box – Blue Box ale w Australii, program na komputer Amiga!
- Silver Box – emulacja klawiszy A, B, C i D – stosowany na liniach wojskowych
- Magenta Box – symulator sygnału wywołania (dzwonienie – generator AC)
- Orange Box – wysyłał kody Caller ID
- >BLOTTO BOX< – APOKALIPSA! W założeniu miał zniszczyć CA
  - oczywiście ten mityczny boks nigdy nie istniał ale wielu o nim mówiło… 8^)
- https://en.wikipedia.org/wiki/Phreaking_boxes

INNE METODY

- War Dialing
  - Znajdowanie “interesujących” numerów
  - Film “War Games” (1983)
  - Wystarczył Apple II, VIC-20 czy C64 i modem akustyczny (300 b/s)



- Calling Cards
  - Karty przedpłacone wykorzystywane zwykle przez podróżujących biznesmenów
  - Istniał Czarny rynek numerów takich kart

ZMIERZCH PHREAKINGU W USA

- „Esquire" – amerykański magazyn dla mężczyzn ukazujący się od 1933 roku.
  - Bet rozkładówek, obecnie nazwalibyśmy go „lajfstajlowym"
- W wydaniu z 1 października 1971 roku ukazał się artykuł „Secrets of the Little Blue Box"
  - https://classic.esquire.com/secrets-of-the-blue-box/
  - Zawierał on opis wykorzysania BB i katastroficzny obraz telekomunikacji w USA...
    - *„So I just punch out KP Zero 44. The Zero is supposed to guarantee a satellite connection and 44 is the country code for England."*
  - Przeczytały go miliony – co oczywiście zaowocowało naśladowcami...
  - Niestety, spowodowało przeczytali go także managerowie kompani telefonicznych, głównie Bell System (monopolisty do 1982 r.)

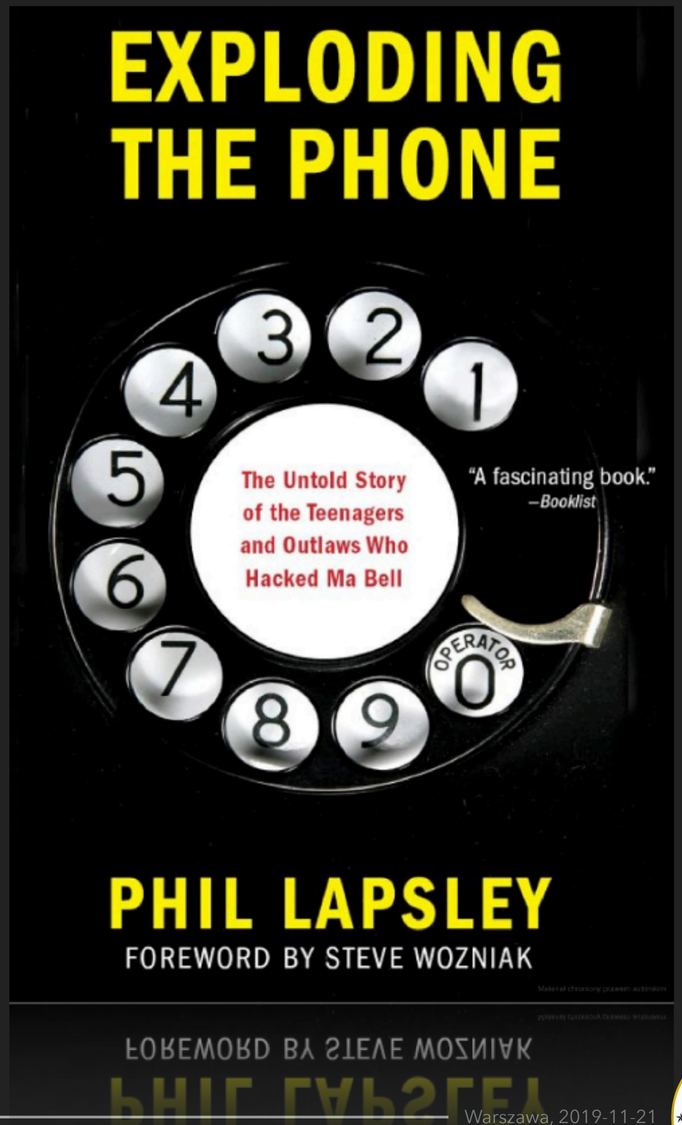
ZMIERZCH PHREAKINGU W USA

- Zainstereowanie policji i służb
- Jednymi ze złapanych za „boksing” byli Steve Woźniak i Steve Jobs... (video)
- FBI zaczęło się interesować tematem już w 1966 roku, gdy wykryto, że BB używali mafiozi
- Przegrana apelacja przed Sądem Najwyższym USA jednego z nich pozwoliła zatrzymywać każdego za tzw. „wire fraud” – marzec 1968
  - Hanna v. United States, 393 F.2d 700 – https://cite.case.law/f2d/393/700/
- W 1974 roku aresztowano Drapera, uznanego za nieformalnego lidera ruchu phreakerów, a potem skazano go za przestępstwa telekomunikacyjne (18 U.S.C. § 1343, tzw. „wire fraud”)
  - W więzieniu Draper przerobił odbiornik radiowy tak, aby monitorować krótkofalówki strażników…
  - Uczył także więźniów podstaw radioamatorstwa oraz... phreakingu

I wciąż myślisz, że jesteś inteligentnym, twardym gościem?!?

POCZTAJ MI...

- EXPLODING THE PHONE – The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell
- Phil Lapsley
- 18,34 zł w Google Books
- Przedmowę napisał Steve Woźniak
- https://books.google.pl/books?id=ECiBd4mYkVwC



Phone Phreaking

a w Polsce?!

Warszawa, 2019-11-21

PHREAKING W POLSCE — RYS HISTORYCZNY

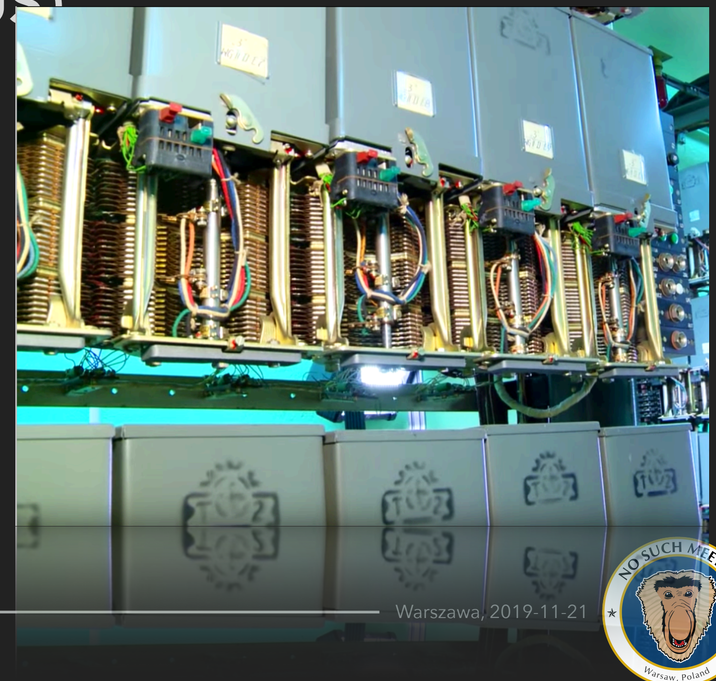
- Początek lat 90-tych, 10,25 abonenta na 100 mieszkańców (1994)
- Dostęp reglamentowany, na założenie linii czekało się kilkanaście lat
- Sieć praktycznie całkowicie analogowa (z wyjątkiem Komertela)
  - sieć była stworzona do obsługi raczkującego biznesu, kier. 039 i nry 3912 w Wawie
  - oparta o centralę 5ESS (AT&T), oferowała usługi cyfrowe ISDN
  - bezpośrednie połączenie międzynarodowe (druga ACMN w Polsce)
- 2 centrale międzynarodowe (od 1993 EACMN w Poznaniu)
- 20 central międzymiastowych*, od 1992 cyfrowe (Katowice EWSD prod. Siemens)
- Rodzaje CA używanych w tym czasie w Polsce (bez ACMM i ACMN):
  - przedwojenny Strowger 32AB – centrala mechaniczna, wybieraki podn.-obr.
  - Pentaconta – j.w., ale oparta na wybierakach krzyżowych a nie dekadowych (1974-)
  - K-65, K-66 – j.w., „rozwinięcie" systemu Pentaconta (1965-)
  - E-10 – elektroniczna, na układach scalonych (1977-)
  - od lat 90-tych EWSD, 5ESS, S12 (Alcatel)– elektroniczne, cyfrowe – no i DTMF!!!
  - i wiele innych, o pojemnościach <1000 NN, szczególnie na wsi i w Wojsku

PHREAKING W POLSCE – POTRZEBY

- Rozliczanie w systemie impulsowym
  - Połączenia lokalne do 1991 roku „kosztowały” 1 impuls,
    Od 1991 roku 1 impuls za 3 minuty połączenia
  - Połączenia międzymiastowe były drogie, rozliczane czasowo – impuls co x sekund
    Jeszcze w latach 80-tych były zamawiane
  - Połączenia międzynarodowe były ASTRONOMICZNIE drogie
    Europa była relatywnie tańsza, w latach 80-tych w większość poł. zamawiana
    poza Europę połączenia realizowała NSS Psary (koło Kielc)
- Zacofana sieć telekomunikacyjna i niska dostępność telefonu
- Brak internetu (dopiero od 1992 r. był dostepny na uczelniach)
- Rozwój sieci modemowej – FidoNet
- Mikrokomputery i „import” oprogramowania
  - Chęć dostępu do warezów
- No i chciało się pogadać, szczególnie między miastami 8^)

PHREAKING W POLSCE – #1 STROWGER BOX

- Stworzony przez Almona Strowgera w 1889 roku
- https://www.youtube.com/watch?v=28Ck0xtr6v8
- Przechodząc obok centrali słychać było charakterystyczny terkot wybieraków
- Każda miała agregat wielkości lokomotywy i akumulatory, co zapobiegało zawaleniu się budynku w chwili utraty zasilania – wybieraki wtedy „siadały"
- Wybieranie wyłącznie pulsowe (dekadowe), pulsy 100-200 ms
  - numery lokalne wybierane były natychmiastowo, bez tzw. „marszruty" (rejestru)
  - charakterystyczne „pływanie" dźwięków w słuchawce (SUS)
- Po pierwszej oraz trzeciej cyfrze „brzęknięcie"
  - to ruch pionowy wybieraka sekcji
- Bio-phreaking
  - właściwie niemożliwy bez ingerencji fizycznej w centralę
  - najlepszy trik – zagięcie blaszki odpowiedzialnej za naliczanie impulsów – robił to „człowiek" z centrali



PHREAKING W POLSCE — #2 PIŁA CITY

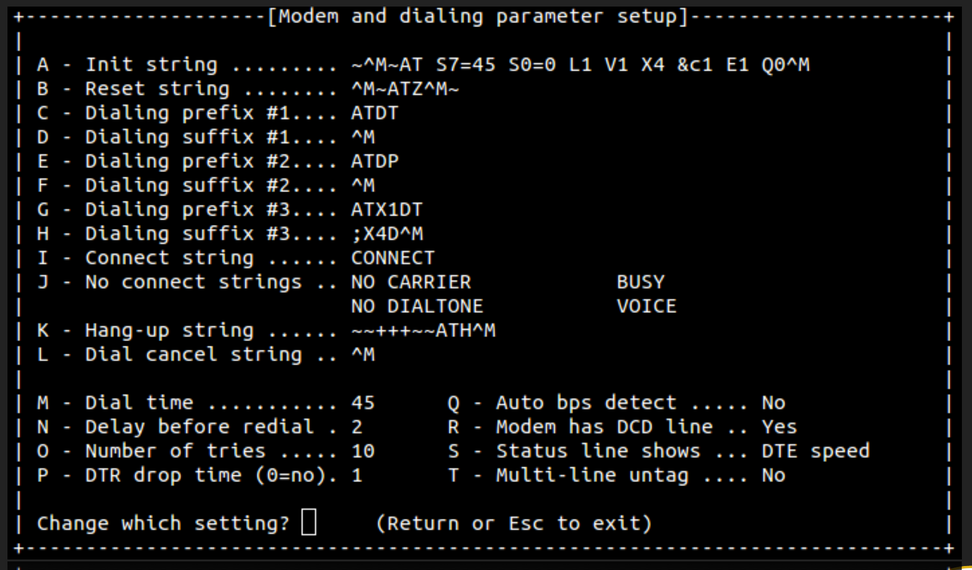
- Numer kierunkowy 065
- Po wybraniu numeru kierunkowego słychać było ciągły ton i można było wybrać numer jakby było się w pięknym mieście Pile
- Czemu zatem nie zadzwonić na zupełnie inny numer, niekoniecznie lokalny?
- ZTCP było to darmowe (brak odwrócenia pęli lokalnej) albo przynajmniej kosztowało tyle, ile rozmowa MM
- Fatalna jakość połączenia
  - Do rozmowy było wystarczające
  - Ledwo chodziła transmisja modemami 2400 bit/s
  - Szybciej tylko z wykorzystaniem modemu US Robotics Courier HST (14400/450)

PHREAKING W POLSCE — PENTACONTA STORIES

- Automatyczna centrala elektromechaniczna oparta na wybierakach krzyżowych
- Nazwa wywodzi się z greckiego 52 – pojemności wybieraków krzyżowych
- Producentem było konsurcjum Francuskich firm LMT i CGCT
- Koncepcja „zainspirowała" polską myśl techniczną – CA K-65 i K-66
- Polska zakupiła licencję na system Pentaconta 1000C 28 września 1972 roku
- Od 1974 roku PC 1000C były produkowane przez Zakłady Wytwórcze Urządzeń Telefonicznych w Warszawie
- Niektóre były wrażliwe na „flash" po wejściu na rejestr ACMM (wybranie 0)
  - Przykład: CA na Dobosza na Ochocie – numery 23[1-8]
  - Po wybraniu zera trzeba było było zadzwonić na numer zamiejscowy, ale taki, który był darmowy lub taryfikowany 1 impulsem (takie były)
  - Szybki „flash" (<200 ms) „zrzucał" abonenta spowrotem na ACMM (jak po 0), skąd można było dalej dzwonić, ale taryfikacja zostaława na 1 lub 0 impulsach
- Ciekawostka: na sygnale wołania bywały przesłuchy (gadki ludzi samych do siebie)

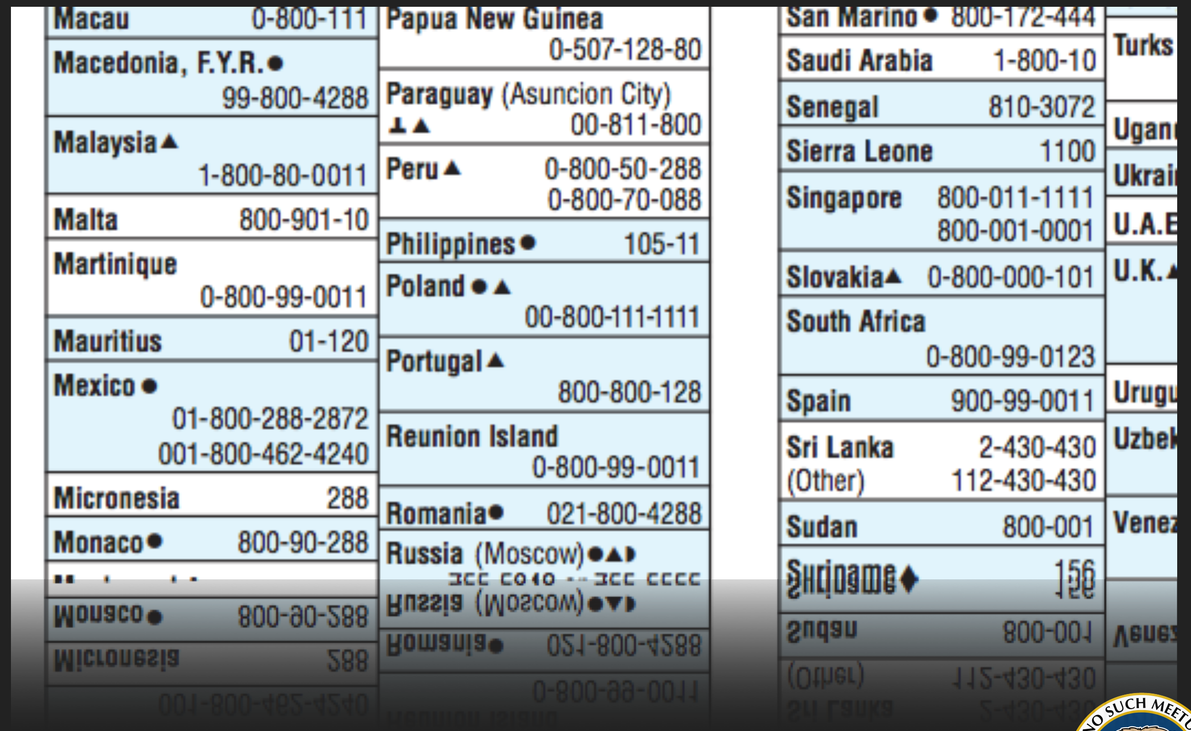
PHREAKING W POLSCE — PANASONIC KTX WELCOME TO

- Centralki firmowe firmy Panasonic – np. KX-TES824
- 8 linii miejskich, 24 linie wewnętrzne
- Zainstalowana karta Direct Inward System Access (DISA) – powitanie, wybieranie numerów wewnętrznych, itd.
- Często na centralkach działało po prostu wybranie „9” podczas powitania i dostawało się „miasto”...
- A jeżeli nie działało, to należało skorzystać z DOMYŚLNYCH kodów serwisowych karty DISA (1111)
  - Skąd my to znamy?...
- Niestety, firmy szybko się orientowały i odcinały dostęp
- Tu pomagał dobry terminal i War Dialing...



PHREAKING W POLSCE – CALLING CARDS...

- Darmowy numer międzynarodowy
  - 00-800-111-1111
  - *„Hello, I would like to charge this call to my calling card…"*
- Skąd zdobywano numery?
  - Zagraniczne BBS-y
  - „Zaufany" człowiek w USA
- Zaczęło się pewnego dnia w Bajtek BBS…
  (tu opowieść kombatancka)



Macau	0-800-111
Macedonia, F.Y.R.●	99-800-4288
Malaysia▲	1-800-80-0011
Malta	800-901-10
Martinique	0-800-99-0011
Mauritius	01-120
Mexico●	01-800-288-2872 001-800-462-4240
Micronesia	288
Monaco●	800-90-288

Papua New Guinea	0-507-128-80
Paraguay (Asuncion City)▲▲	00-811-800
Peru▲	0-800-50-288 0-800-70-088
Philippines●	105-11
Poland●▲	00-800-111-1111
Portugal▲	800-800-128
Reunion Island	0-800-99-0011
Romania●	021-800-4288
Russia (Moscow)●▲◗	

San Marino●	800-172-444
Saudi Arabia	1-800-10
Senegal	810-3072
Sierra Leone	1100
Singapore	800-011-1111 800-001-0001
Slovakia▲	0-800-000-101
South Africa	0-800-99-0123
Spain	900-99-0011
Sri Lanka (Other)	2-430-430 112-430-430
Sudan	800-001
Suriname♦	156

PHREAKING W POLSCE – SOFT PORN STYLE

- Dziwne numery TPSA
  - 0-212212
  - 0-212638
  - 0-212640
  - Po połączeniu słychać było ciągły ton i można było dzwonić dalej...
  - Często znikały, stąd całe 0-212 czesane było war dialerami (wystarczało <8 h)
- Ekstendery:
  - Albrecht Polska
    - 080068046
  - Prokom oddział w Łodzi
    - 080068035 - „9” + numer (2 miesiące aktywne)
- Nieznane:
  - 6230011 (Warszawa)
  - 6295937 – nieokreślony instytut w Warszawie, reagował na wybranie „9” i kod
  - 1111 (to chyba Panasonic KTX)
- Straz miejsca Gminy Centrum:
  - 6368378 – 9+1111...

PHREAKING W POLSCE – KUNG FU STYLE

- Trzeba było wyłowić linię jakiegoś przedsiębiorstwa i podpiąć się nocą krokodylkami
- Nocka w Ministerstwie
  - Miejską legendą jest to, że tym sposobem do Polski trafiły pierwsze Windows 3.0 – z użciem modemu Courier HST – dostępne potem na Grzybowskiej
- Nocka na Centrali Abonenckiej
  - Najlepiej Strowger, bo w prosty sposób można było się wpiąć w linię
  - Połączenia nie były trafyfikowane, tzn. nie trafiały do „systemu bilingowego” czyli fizycznych liczników abonenckich, których całe sekcje były w osobnym pokoju
  - Zestaw 386SX 4 MB RAM + DesqView 2.0 + karta 2xUART 16550 do tego dwa modemy zewnętrzne i jeden w formie karty (V.32 9600) – trzy sesje Telix (DOS)
  - No i dużo kawy...

PHREAKING W POLSCE – URMET STYLE

- Aparaty publiczne produkowane przez włoską firmę Urmet (przetarg TPSA w 1991)
- Niebieski TSP-91
  - obsługa kart magnetycznych z zapisaną liczbą impulsów (25, 50, 100)
  - procesor Motorola 68HC11, 64 KB ROM
- Trik na „rozmowę przychodzącą”
  - Zadzwonić do budki, rozłączyć się i szybko odebrać – dostawało się wolną, bezpłatną linię
- Trik 0-800
  - Po wybraniu 4 cyfr czekamy, wciskamy „1” i można dzwonić dalej (za darmo)
- Reverse engineering
  - W 2001 roku pojawił sie „wsad” do EPROM-ów, który stosownie modyfikował zachowanie automatu, wystarczyło tylko otworzyć aparat i podmienić kostkę ROM

PHREAKING W POLSCE – URMET STYLE

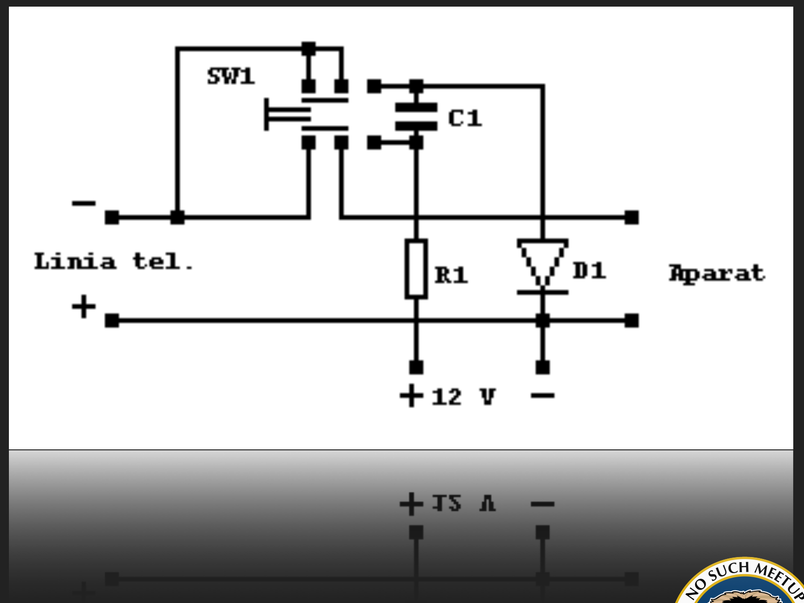
- Srebrny TPE-97/U
  - montowany od 1998 roku
  - obsługa kart czipowych (mało popularne) i magnetycznych
  - solidniejszy od niebieskiego, lepszy procesor
  - wbudowany modem 2400 do zdalnej aktualizacji
  - lepsze zabezpieczenie fizyczne – trudne do sforsowania
- Trik 974
  - włóż kartę z min. 1 impulsem
  - wybierz numer 974
  - wciśnij przycisk [FC]
  - po pojawieniu się ciągłego sygnału wybierz 997 (centrala ignoruje ten numer)
  - podczas wybierania 997 automat pocharczy, postrzela w słuchawkę, a po kilku sekundach wrzuci nam „zajętość”
  - po tej zajętości znowu mamy ciągły sygnał i wybieramy normalnie z klawiatury aparatu
- W latach 2000 opracowano sposób przejęcia – udawane centrum serwisowe...

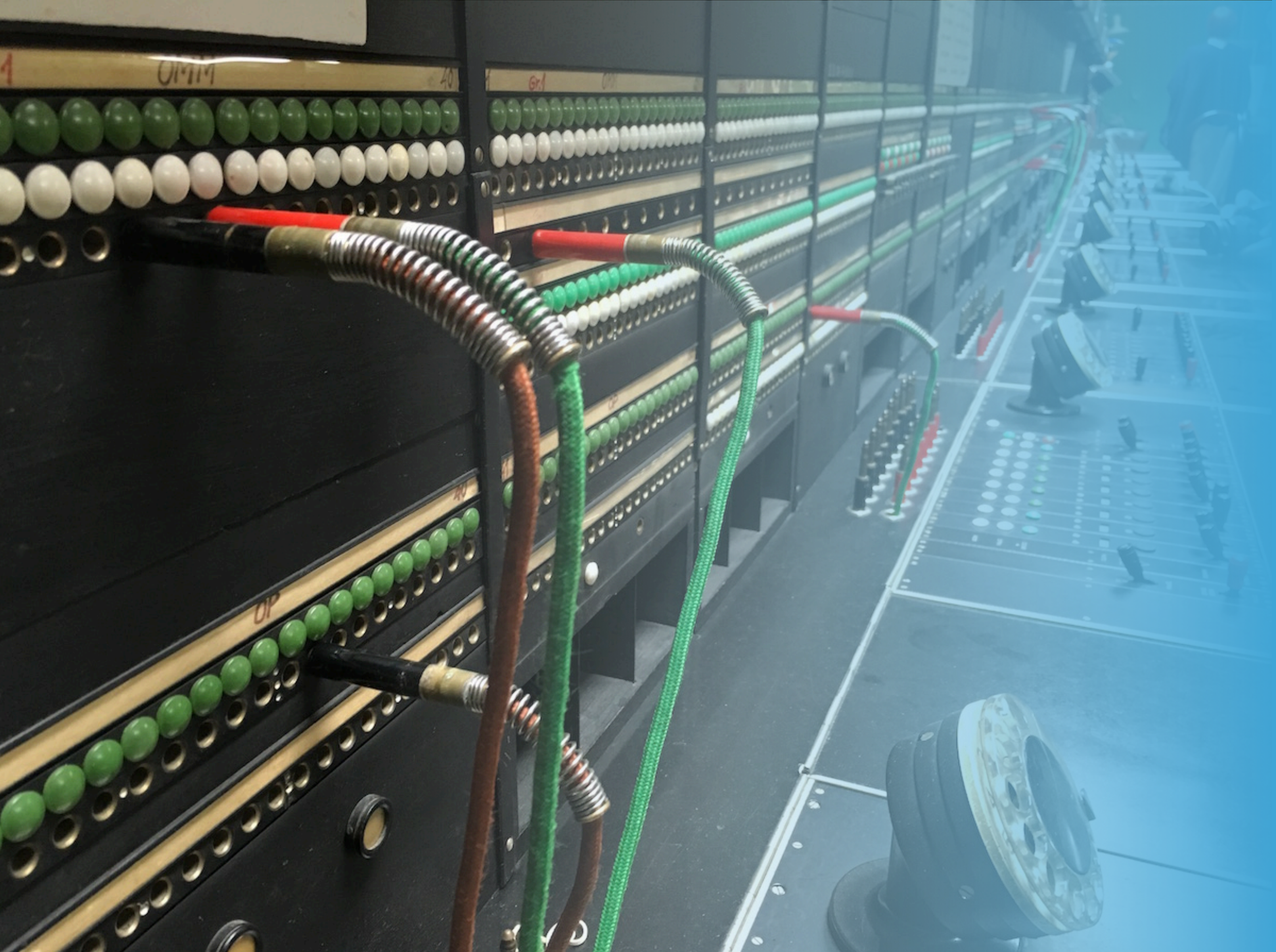
PHREAKING W POLSCE – HACKING 5ESS

- Centrale cyfrowe też można było „wykorzystać” do swoich celów
- Polscy phreakerzy wykorzystywali podatności związane z niechlujną konfiguracją
  - Znajdź numer aparatu telefonicznego w budce – często był na nim naklejony
  - Wprowadź bezwarunkowe przekierowanie w formacie *21*numer# (np. numer Kasi Figury na 0-700), które zwykle trzeba było włączyć podaniem do TPSA
  - Z innego aparatu zadzwoń na numer budki – a połączysz się z linią 0-700
- Po wyłączeniu tej „usługi" na Żoliborzu z Dyrekcji Okręgu w Polskę poszedł faks do wszystkich central 5ESS by natychmiast się zabezpieczyli – 5ESS była dostarczana z fabryki z włączonymi takimi usługami
  - Nie mniej, ten faks nie dotarł do miejsc, gdzie instalowano nowe centrale 5ESS, na które TPSA masowo wymieniała stare Pentaconty i Strowgery, więc co chwilę okazywało się, że „da się” ale np. w Siedlcach albo Radomiu...
  - „*Nasze zamiłowanie do letnich przejażdżek po woj. Mazowieckim nadal odbija się czkawką Narodowego Operatora ludzkich portfeli.*”

PHREAKING W POLSCE – DARMOFON BOX

- **Proste urządzenie wpinane w linię telefoniczną, które maskowało podniesienie słuchawki**
- **„***Dzwoni telefon. W czasie przerwy pomiędzy dzwonkami wcisnąć isostat. Po chwili przekaźnik zaskoczy i mrugnie dioda LED. Wtedy podnieść słuchawkę, i można prowadzić rozmowę, która jest bezpłatna.***”**
- **Działało na centralach Pentaconta i (z modyfikacjami) na centralach K-66, m. in.**
  - **610 (Gocławek), 633 (Broniewskiego), 635 (Muranów), 818 (Ząbkowska), 849 (Mokotów III), 678/679 (Targówek), 667 (Ursus)...**
  - **Ciekawostka: ostatnia centrala analogowa pracowała do 2005 roku miejscowości Skorogoszcz, gmina Lewin Brzeski, województwo opolskie**
- **My zatem też mieliśmy swoje „boksy” i zdolnych ludzi**
- **Ale przyszedł internet i te wszystkie spajpaje...**





FIN

NO SUCH MEETUP

Warsaw, Poland