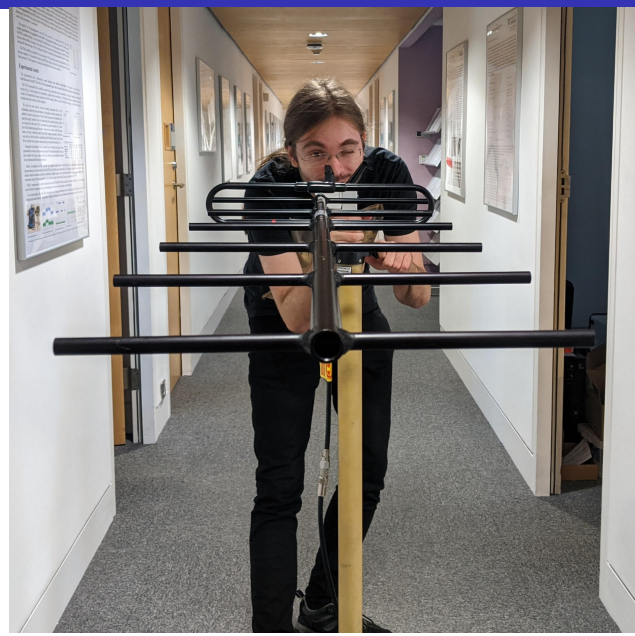
Side-channel security requirements for electronic voting equipment

Markus G. Kuhn, Dimitrije Erdeljan

Department of Computer Science and Technology
University of Cambridge



Do TEMPEST-style attacks matter in the real world?



"TEMPEST-style attack" =

- *Passive* electromagnetic eavesdropping
- on *unintentional* emissions
  (i.e., not radio broadcasts, spyware modulating covert channels)
- at distances in the ≈2–200 metre range
  (e.g., from neighbour room, neighbour building, public spaces)
- covert presence of adversary
- target device not under control of adversary
- mainly targeting communications cables and peripherals
  (displays, keyboards, printers, serial ports, etc.)
- the sort of threat NATO SDIP-$\{27, 28, 29\}$ and similar "TEMPEST" standards presumably aim to address

As opposed to:

- side-channel attacks against cryptographic algorithms
- probes within millimetres from the chip surface in a lab

Electronic voting machines in the Netherlands

Direct-recording electronic (DRE) voting machines
$\rightarrow$ longstanding integrity/verifiability concerns

October 2006: "Wij vertrouwen stemcomputers niet" report

RF eavesdropping demonstration on Nedap ES3B voting machine





Rop Gonggrijp, Willem-Jan Hengeveld, et al.; USENIX Electronic Voting Technology 2007
`https://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf`
`https://web.archive.org/web/20170822114757/http://wijvertrouwenstemcomputersniet.nl/`
`https://www.youtube.com/watch?v=B05wPomCjEY`

Nedap ES3B radio-frequency vulnerability details

- 4×40 character dot-matrix LCD
- each two lines driven by Hitachi HD44780 LCD controller
- LCD controller available in two versions:
  - Japanese: katakana font
  - European: ISO 8859-1 + Greek + Cyrillic font
- Nedap ES3B uses . . .

Nedap ES3B radio-frequency vulnerability details

- 4×40 character dot-matrix LCD
- each two lines driven by Hitachi HD44780 LCD controller
- LCD controller available in two versions:
  - Japanese: katakana font
  - European: ISO 8859-1 + Greek + Cyrillic font
- Nedap ES3B uses . . . the Japanese version
- non-ASCII characters need to be uploaded as bitmap
- display updated in endless loop, periodically at 72 Hz

Nedap ES3B radio-frequency vulnerability details

- 4×40 character dot-matrix LCD
- each two lines driven by Hitachi HD44780 LCD controller
- LCD controller available in two versions:
  - Japanese: katakana font
  - European: ISO 8859-1 + Greek + Cyrillic font
- Nedap ES3B uses . . . the Japanese version
- non-ASCII characters need to be uploaded as bitmap
- display updated in endless loop, periodically at 72 Hz
- display of one non-ASCII character drops loop frequency to 58 Hz
- Christen Democratisch Appèl (CDA)
- loop-frequency audible as 72/58 Hz buzz with radio at several frequencies in the 36–150 MHz range → CDA detector



`https://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf`

Nedap ES3B radio-frequency vulnerability impact

The Nedap ES3B vulnerability seemed easy to fix in software: update display only when needed, to remove periodic buzz.

But this eavesdropping demonstration caused significant public interest.

(Unlike the many other serious concerns previously raised about the unverifiable integrity of DRE voting machines!)

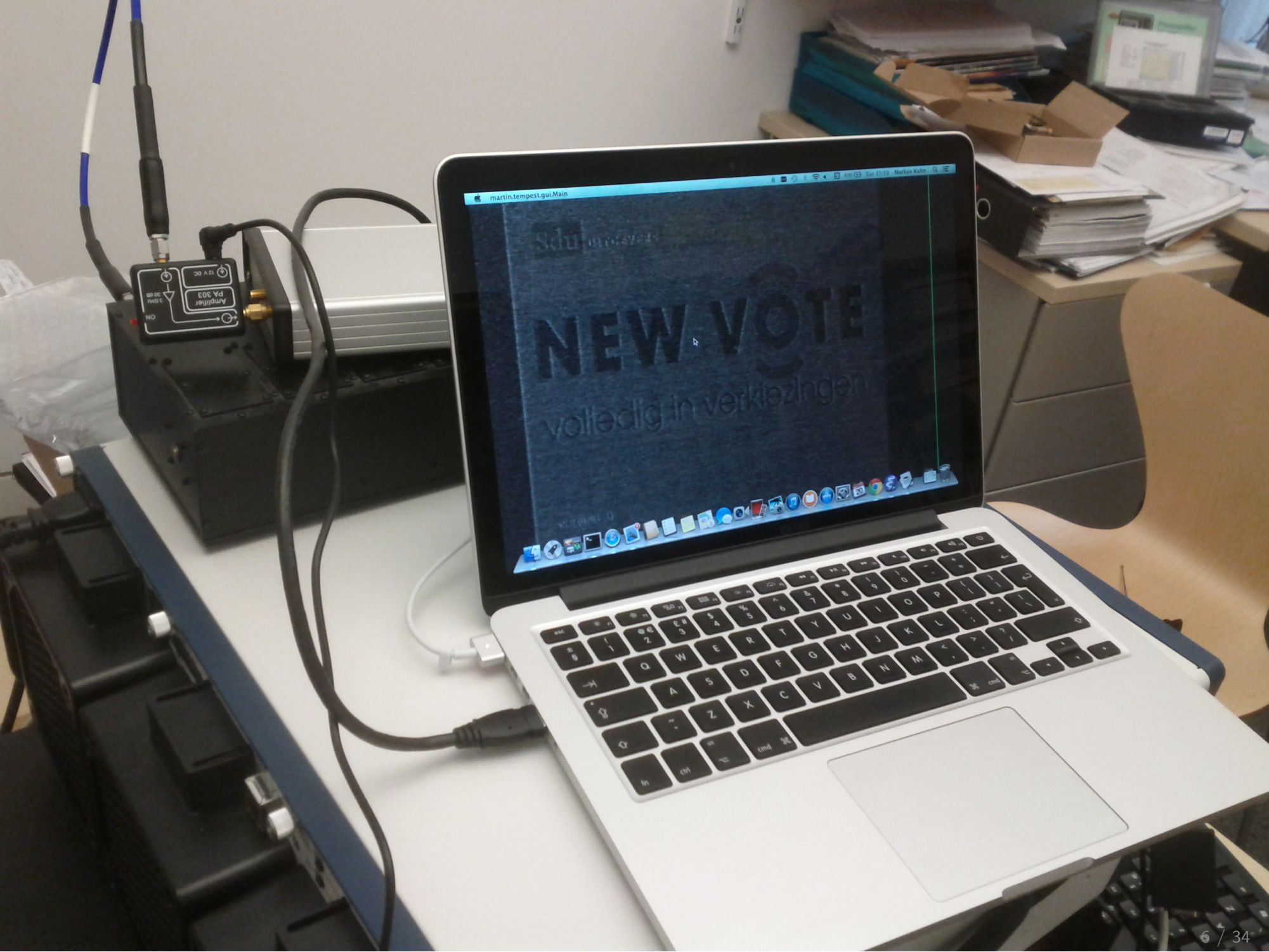
Secrecy of the vote is an essential requirement of Dutch elections.

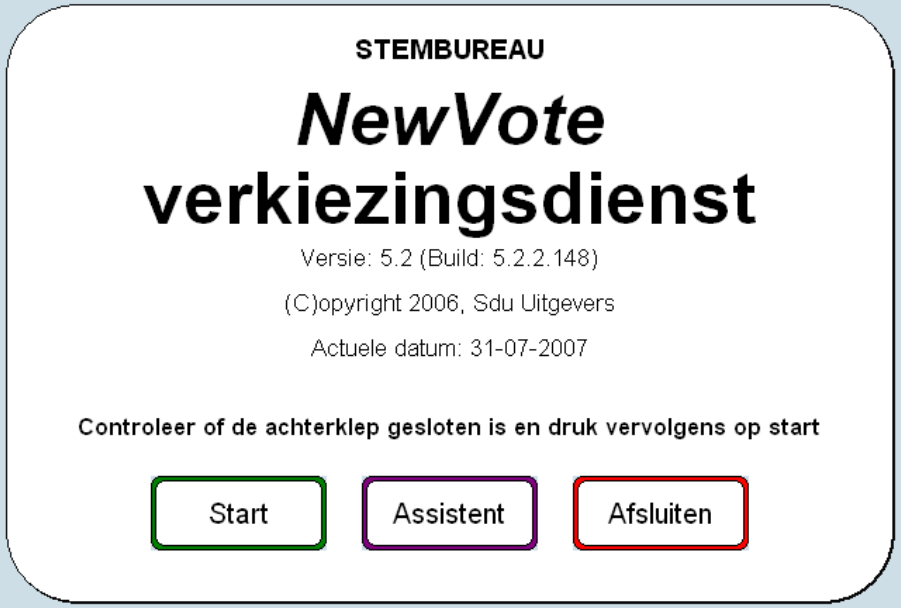
Dutch General Intelligence and Security Service (AIVD) tested in October 2006 a second DRE machine in use at the time.

AIVD reported video emissions distinguishable up to 30–40 metres.

Two out of two voting machines tested had a TEMPEST-style problem!




martin.tempest.gui.Main
NEW VOTE
volledig in verkiezingen


STEMBUREAU
NewVote
verkiezingsdienst
Versie: 5.2 (Build: 5.2.2.148)
(C)opyright 2006, Sdu Uitgevers
Actuele datum: 31-07-2007
Controleer of de achterklep gesloten is en druk vervolgens op start
Start
Assistent
Afsluiten


NewVote verkiezingsdienst
STEMBUREAU
NewVote
verkiezingsdienst
Versie: 5.2 (Build 5.2.2.148)
(C)opyright 2006, Sdu Uitgevers
Actueel tot en met 01-01-2001
Controleer of de echte stemcomputer is aangesloten voordat u verder gaat
Start
Assistent
Afsluiten


NewVote verkiezingsdienst
STEMBUREAU
NewVote
verkiezingsdienst
Versie 5.2 (Build 5.2.2148)
(C)opyright 2001 Sdu Uitgevers
Actuele datum 01-01-2001
Controleer of de achterklep gesloten is en druk vervolgens op start
Start
Assistent
Afsluiten

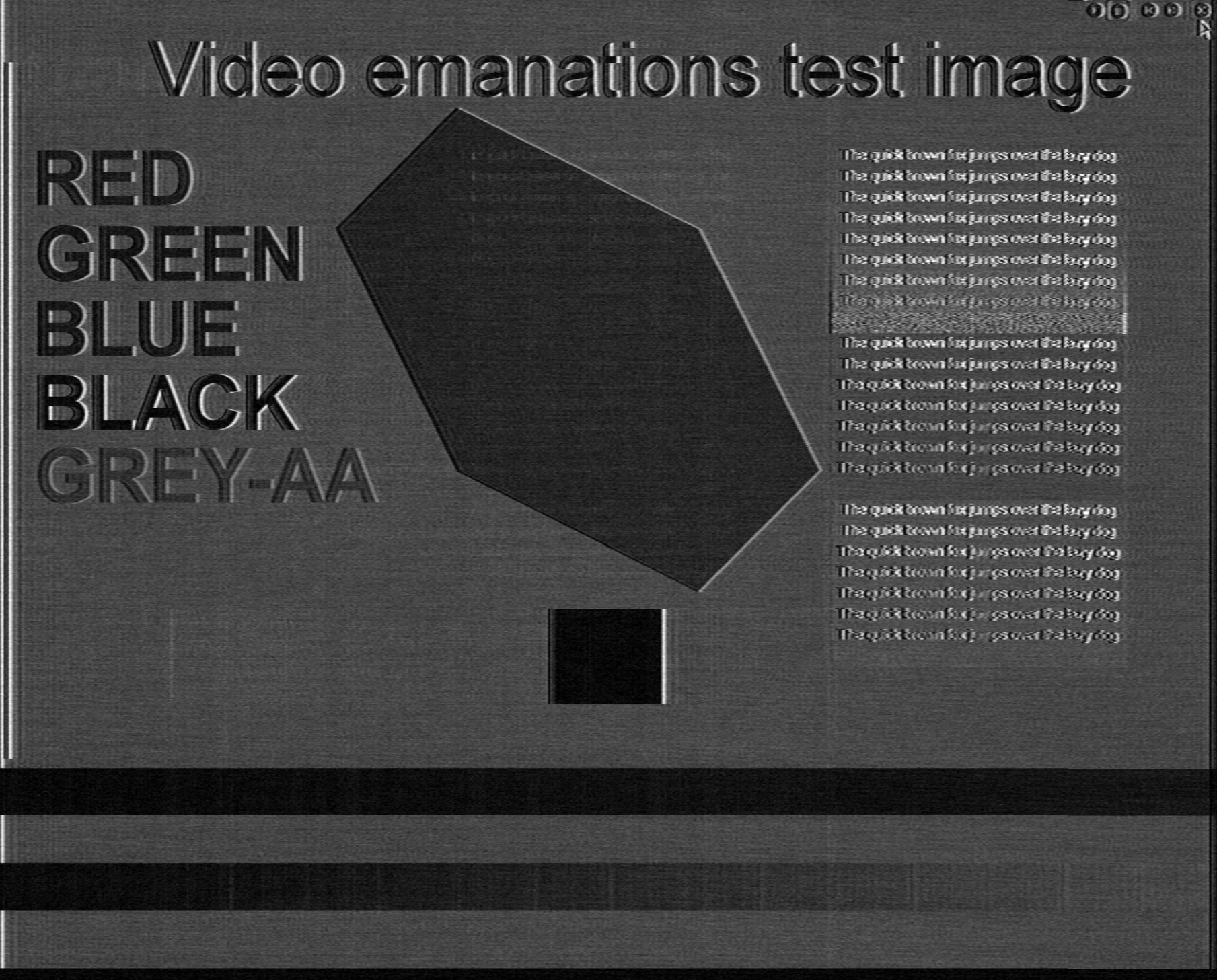

NewVote verkiezingsdienst
STEMBUREAU
NewVote
verkiezingsdienst
Versie 5.2 (Build 5.2.2148)
(C)opyright 2001 Sdu Uitgevers
Actuele datum 01-01-2001
Controleer of de achterklep gesloten is en druk vervolgens op start
Start
Assistent
Afsluiten

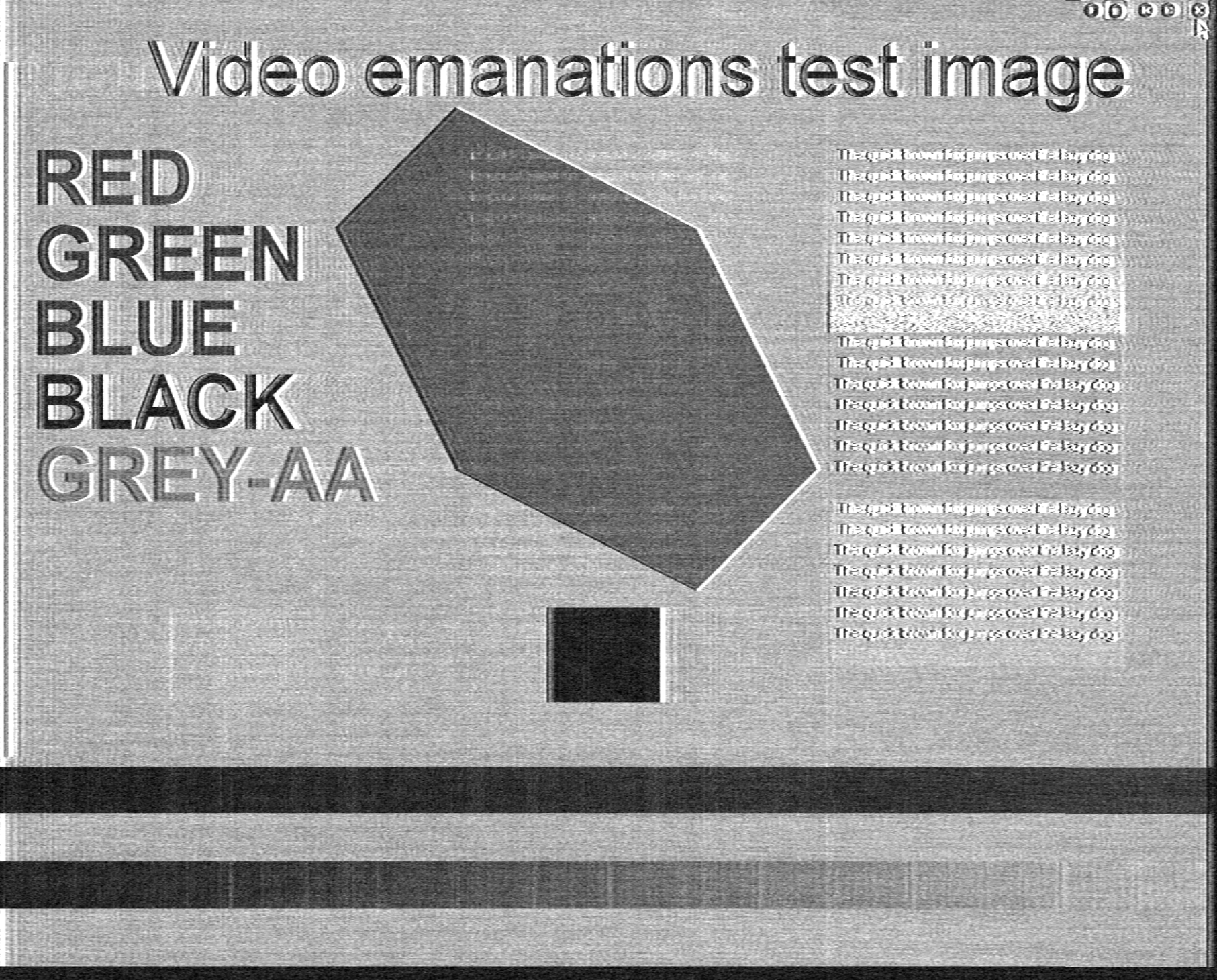
Video emanations test image

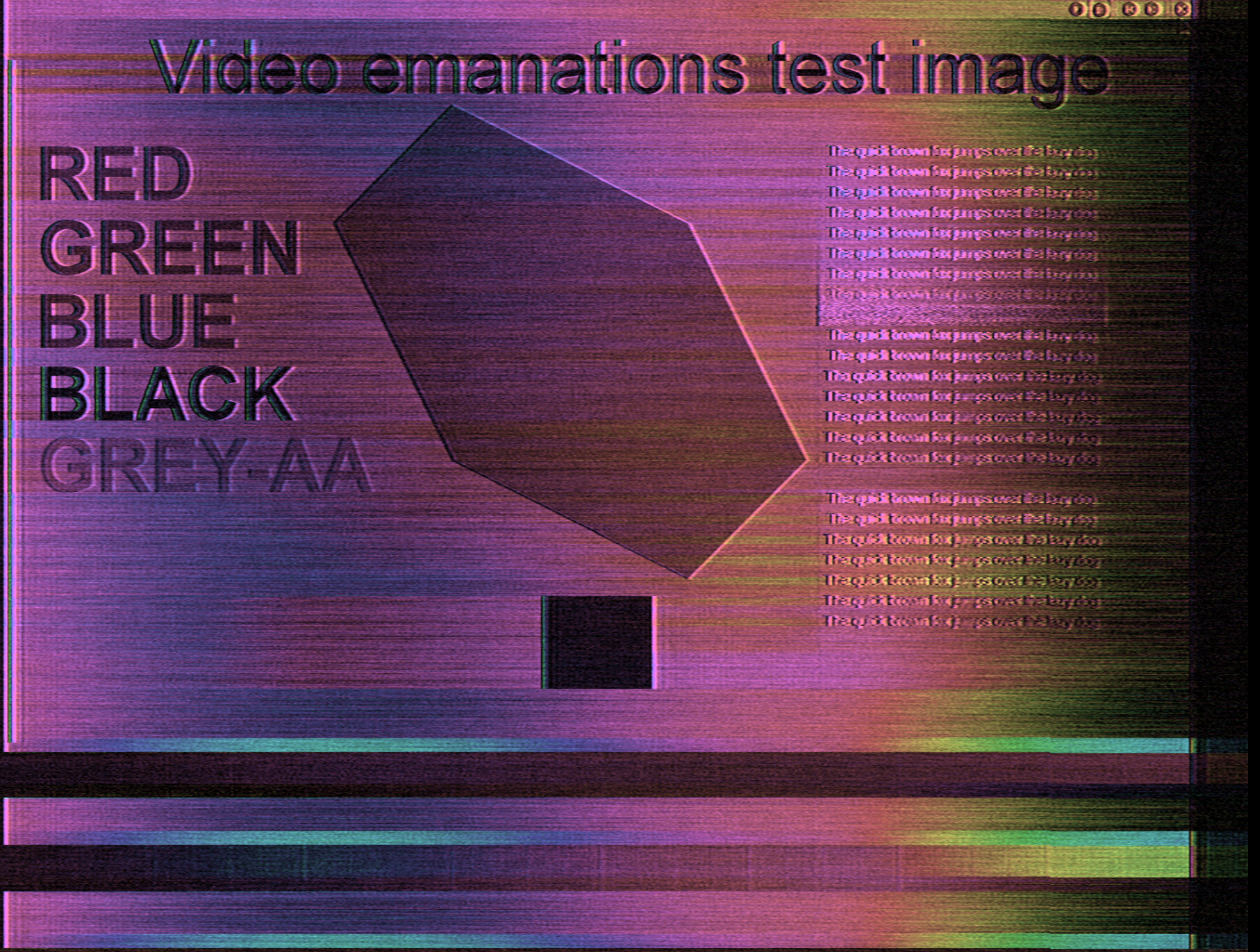
RED
GREEN
BLUE
BLACK
GREY-AA



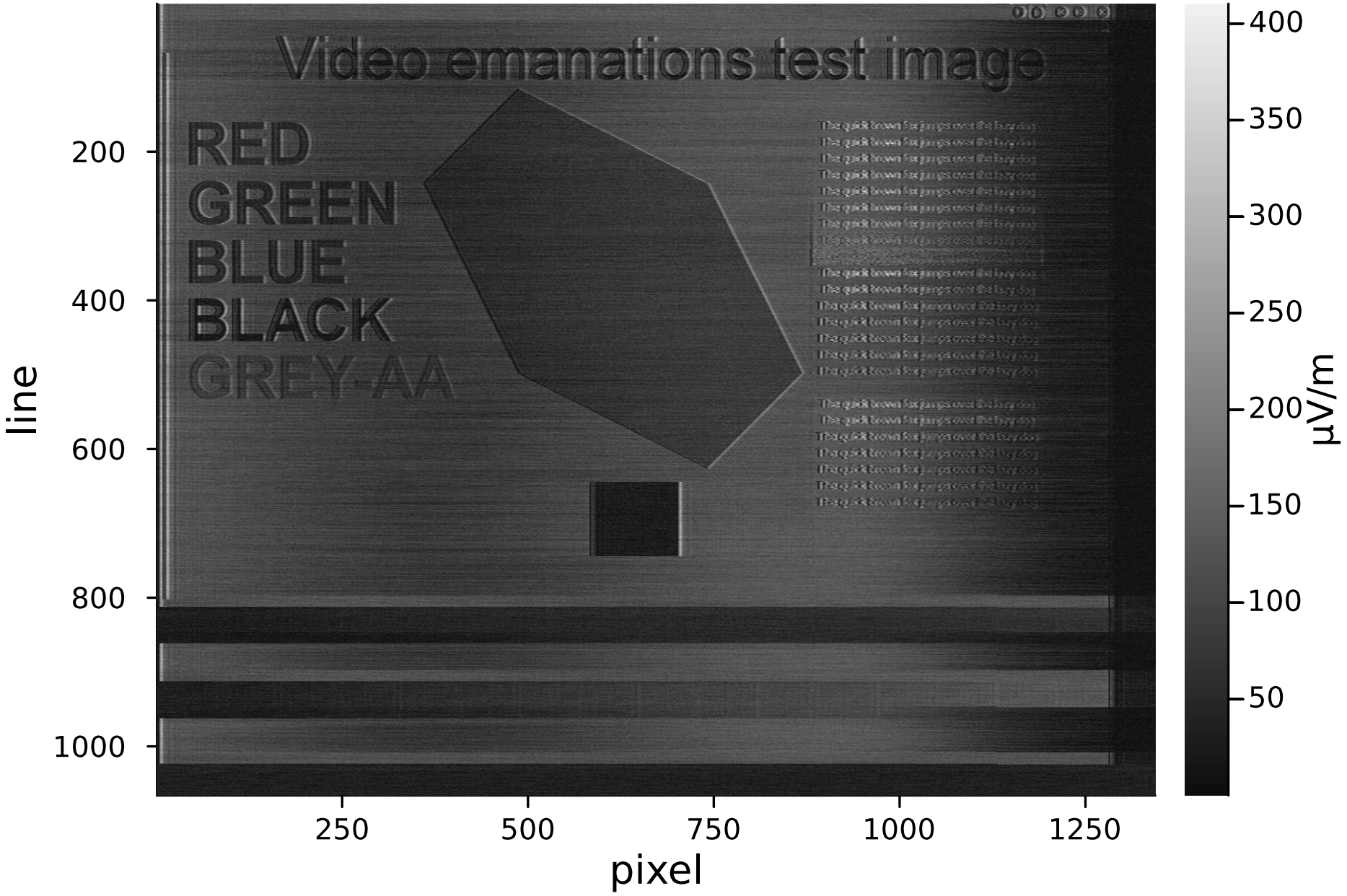
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog


Video emanations test image
RED
GREEN
BLUE
BLACK
GREY-AA
The quick brown fox jumps over the lazy dog

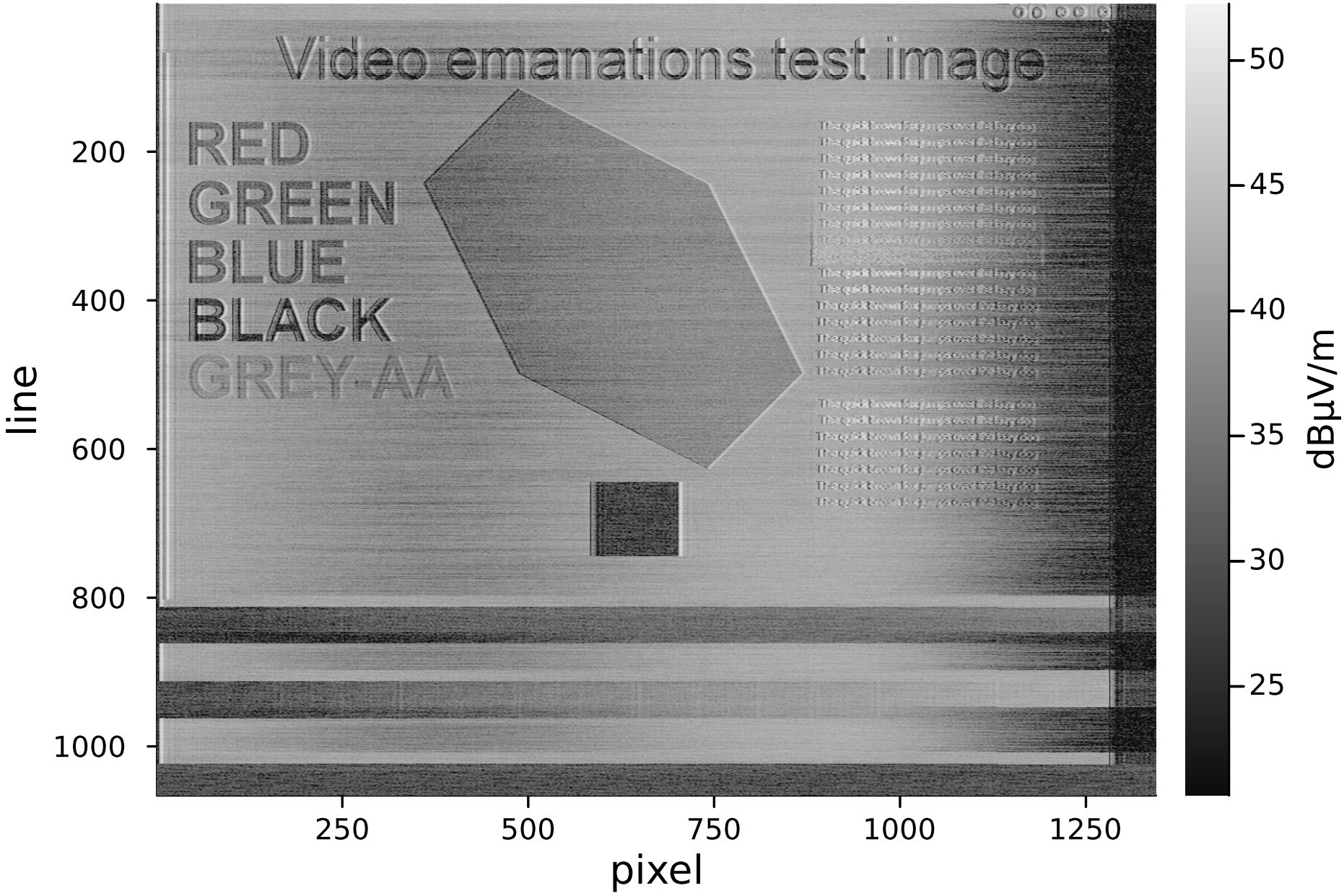

Video emanations test image
RED
GREEN
BLUE
BLACK
GREY-AA


Video emanations test image
RED
GREEN
BLUE
BLACK
GREY-AA

E-field at 2 m, 40 MHz bandwidth



E-field at 2 m, 40 MHz bandwidth

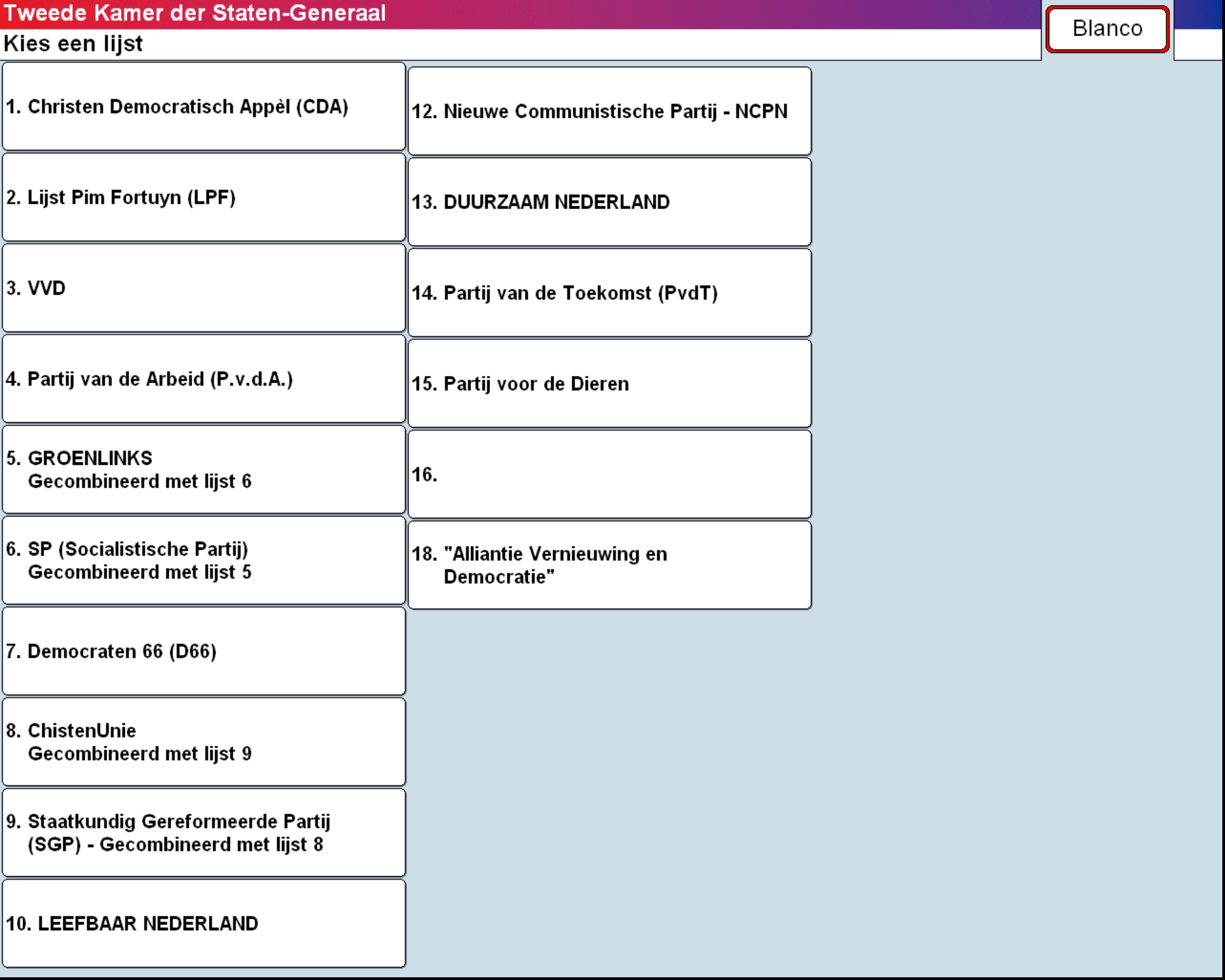


Comparison with background noise levels

40 MHz bandwidth, low UHF band:

Source	μV/m	dBμV/m
previous video signal @ 2 m	200–400	46–52
previous video signal @ 20 m	20–40	26–32
RMS noise in my office	98	40
same after 100 kHz bandstop filter	64	36
thermal noise on a dipole	32	30
ITU P.372 radio noise (>300 MHz)	35–200	31–46

- field strength drops linearly with distance
- noise drops with square root of number of frames averaged
  average e.g. 1 second = 60 frames ≈ 8× (18 dB) better SNR
- directional antenna: 10–15 dBd gain


Tweede Kamer der Staten-Generaal
Blanco
Kies een lijst
1. Christen Democratisch Appèl (CDA)
2. Lijst Pim Fortuyn (LPF)
3. VVD
4. Partij van de Arbeid (P.v.d.A.)
5. GROENLINKS
Gecombineerd met lijst 6
6. SP (Socialistische Partij)
Gecombineerd met lijst 5
7. Democraten 66 (D66)
8. ChistenUnie
Gecombineerd met lijst 9
9. Staatkundig Gereformeerde Partij
(SGP) - Gecombineerd met lijst 8
10. LEEFBAAR NEDERLAND
12. Nieuwe Communistische Partij - NCPN
13. DUURZAAM NEDERLAND
14. Partij van de Toekomst (PvdT)
15. Partij voor de Dieren
16.
18. "Alliantie Vernieuwing en
Democratie"

1. Christen Democratisch Appèl (CDA) - Kies een kandidaat

Herstel

1. **Balkenende** J.P. (Jan Peter) (m) Capelle a/d IJssel	17. **van Oerle-van der Horst** N.W. (Niny) (v) Haarlem	33. **Mastwijk** J.J. (Jan) (m) Hoogeveen	49. **van Dijk** J.J. (Jan Jacob) (m) Culemborg	65. **Smulders** J.C.G.J. (Hans) (m) Asten
2. **van der Hoeven** M.J.A. (Maria) (v) Maastricht	18. **Mosterd** A. (Aart) (m) Putten	34. **Koopmans** G.P.J. (Ger) (m) Velden	50. **Eski** N. (Nihat) (m) Utrecht	66. **Visser** M.K. (Martine) (v) Groningen
3. **Verhagen** M.J.M. (Maxime) (m) Voorburg	19. **Schreijer-Pierik** J.M.G. (Annie) (v) Hengevelde	35. **Rambocus** N. (Nirmala) (v) Utrecht	51. **Omtzigt** P.H. (Pieter) (m) Borne	67. **Weigand-Timmer** H.A.C. (Jet) (v) Culemborg
4. **Ross-van Dorp** C.I.J.M. (Clémence) (v) Breedenbroek	20. **van Bochove** B.J. (Bas Jan) (m) Lelystad	36. **Ormel** H.J. (Henk Jan) (m) Hengelo (Gld)	52. **Brinkel** T.B.F.M. (Theo) (m) Leidschendam	68. **Beuckens-Vries** M. (Martha) (v) Dordrecht
5. **van Geel** P.L.B.A. (Pieter) (m) Helmond	21. **Joldersma** F. (Cisca) (v) Tilburg	37. **Spies** J.W.E. (Liesbeth) (v) Alphen a/d Rijn	53. **van Hijum** Y.J. (Eddy) (m) Zwolle	69. **Haitsma** F.S. (Foka) (v) Goutum
6. **Verburg** G. (Gerda) (v) Woerden	22. **van Haersma Buma** S. (Sybrand) (m) Voorburg	38. **Hessels** J.W.M.M.J. (Jos) (m) Montfort	54. **Jonker** C.W.A. (Corien) (v) Maarheeze	70. **Cornelisse-Putter** E.C.M. (Elly) (v) Uitgeest
7. **Atsma** J.J. (Joop) (m) Surhuisterveen	23. **de Haan** H. (Henk) (m) Lettelbert	39. **Vietsch** C.A. (Antoinette) (v) Utrecht	55. **Willemse-van der Ploeg** A.A.M. (Ans) (v) Heiloo	71. **Zomer** H. (Han) (m) Vriezenveen
8. **Ferrier** K.G. (Kathleen) (v) Leusden	24. **van de Camp** W.G.J.M. (Wim) (m) 's-Gravenhage	40. **de Vries** J.M. (Jan) (m) Goudriaan	56. **Knops** R.W. (Raymond) (m) Horst	72. **Bastiaansen** C.A.J. (Carla) (v) Tilburg
9. **Wijn** J.G. (Joop) (m) Amsterdam	25. **van Vroonhoven-Kok** J.N. (Nicolien) (v) 's-Gravenhage	41. **Jager** H. (Rikus) (m) Appingedam	57. **Donders-de Leest** M.J.D. (Rianne) (v) Etten-Leur	73. **Geluk-Poortvliet** L.W.D. (Lenny) (v) Burgh-Haamstede
10. **Rietkerk** T.W. (Theo) (m) Kampen	26. **ten Hoopen** J. (Jan) (m) Zoetermeer	42. **Bruls** H.M.F. (Hubert) (m) Nijmegen	58. **Simonse** H.R. (Hennie) (v) Emmeloord	74. **Crooijmans** M.J.A. (Maud) (v) Beesel
11. **Buijs** S. (Siem) (m) Goes	27. **Sterk** W.R.C. (Mirjam) (v) Utrecht	43. **Algra** R.H. (Rendert) (m) Jubbega	59. **Kempen-van Dommelen** G.J.M. (Gerda) (v) Nijmegen	75. **van der Veen** A.M. (Arie) (m) Deventer
12. **Eurlings** C.M.P.S. (Camiel) (m) Valkenburg (L)	28. **van Lith** M.T.J.M. (Erik) (m) Geffen	44. **Haverkamp** M.C. (Maarten) (m) Nederhorst den Berg	60. **Kamp** A.J. (Ton) (m) Hengelo (O)	
13. **Meijer** T.A.M. (Theo) (m) Nistelrode	29. **de Pater-van der Meer** M.L. (Marleen) (v) Zutphen	45. **Aasted-Madsen-van Stiphout** J.D.M.P. (Ine) (v) Kerkrade	61. **Mes** H.J. (Henk) (m) 's-Gravenzande	
14. **van Ardenne-van der Hoeven** A.M.A. (Agnes) (v) Vlaardingen	30. **van Winsen** B.P.J. (Bart) (m) Haaksbergen	46. **van Fessem** W.M.M. (Wim) (m) Breda	62. **Kuiper** C.K. (Corina) (v) Veldhoven	
15. **Çörüz** C. (Coskun) (m) Haarlem	31. **de Nerée tot Babberich** F.J.F.M. (Frans) (m) Leefdaal (B)	47. **van Loon-Koomen** M.G.E. (Myra) (v) Ossenisse	63. **Verheijen** J.A.G. (Joost) (m) Gouda	
16. **van der Knaap** C. (Cees) (m) Rotterdam	32. **Kortenhorst** R.W.F. (Roland) (m) Joure	48. **Smilde** M.C.A. (Margreeth) (v) Eelde	64. **Bolhuis** C.A.P. (Alex) (m) Epe	

Herstel

6. SP (Socialistische Partij) Gecombineerd met lijst 5 - Kies een kandidaat

1. **Marijnissen** J.G.C.A. (Jan) (m) Oss	11. **Slutzky** A. (Alejandra) (v) Amersfoort	21. **van Gerven** H.P.J. (Henk) (m) Oss
2. **Kant** A.C. (Agnes) (v) Doesburg	12. **Irrgang** E. (Ewout) (m) Amsterdam	22. **Haan** Y.J. (Yorick) (m) Schiedam
3. **van Bommel** H. (Harry) (m) Amsterdam	13. **van Heijningen** J.G.C. (Hans) (m) Amsterdam	23. **Erciyas** M. (Mahmut) (m) Oss
4. **de Wit** J.M.A.M. (Jan) (m) Heerlen	14. **Roovers** R.C.J. (René) (m) Dongen	24. **Elzinga** A. (Tuur) (m) Haarlem
5. **van Velzen** K. (Krista) (v) 's-Gravenhage	15. **van Gijlswijk** L.R. (Rosita) (v) Groningen	25. **Geurts** P.J.J.M. (Paul) (m) Horst a/d Maas
6. **de Ruiter** P. (Piet) (m) Delft	16. **Dekker** I. (Ingrid) (v) Delft	26. **Boorsma** R.K. (Ronald) (m) IJlst
7. **Lazrak** A. (Ali) (m) Amsterdam	17. **van Dijk** J.J. (Jasper) (m) Amsterdam	27. **Baron** F. (Frans) (m) Drachten
8. **Vergeer-Mudde** F. (Fenna) (v) Leiden	18. **Harmes** G.W.A.M. (Gerard) (m) Alphen a/d Rijn	28. **Zondag** G. (Geert) (m) Veenoord
9. **Gerkens** A.M.V. (Arda) (v) Haarlem	19. **Palm** B.T.H.M. (Ineke) (v) Rotterdam	29. **Palmen-Lehmann** J.F. (Hanny) (v) Ferwert
10. **Vankan** H.C.H. (Hubert) (m) Kerkrade	20. **Jankie** C. (Chandra) (v) Hoofddorp	30. **Sciacca-Noordhuis** C. (Corry) (v) Spijk (Gn)

U heeft gekozen voor

1. Christen Democratisch Appèl (CDA)

1. Balkenende
J.P. (Jan Peter) (m)
Capelle a/d IJssel

Akkoord

Herstel

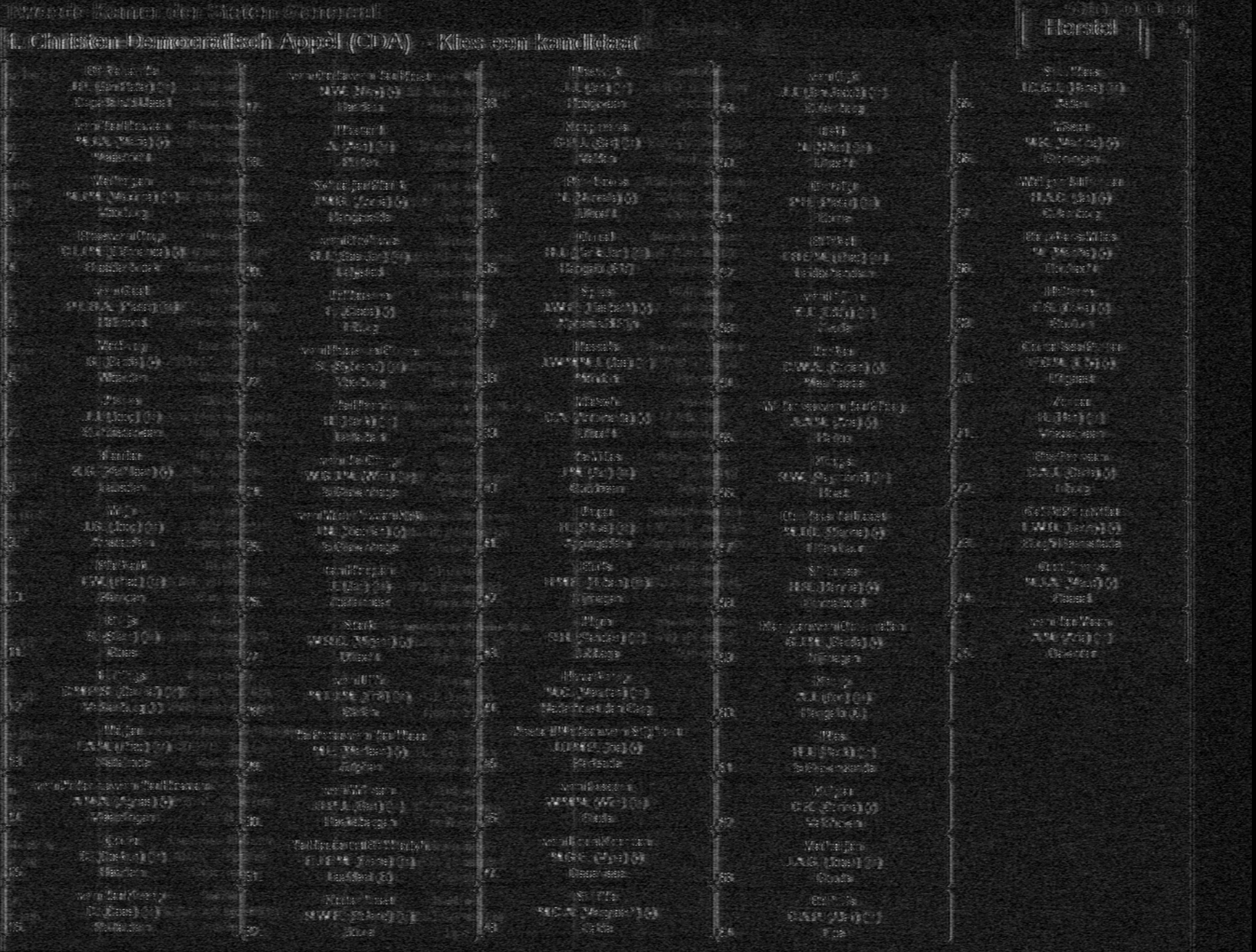
U heeft gekozen voor

6. SP (Socialistische Partij)
Gecombineerd met lijst 5

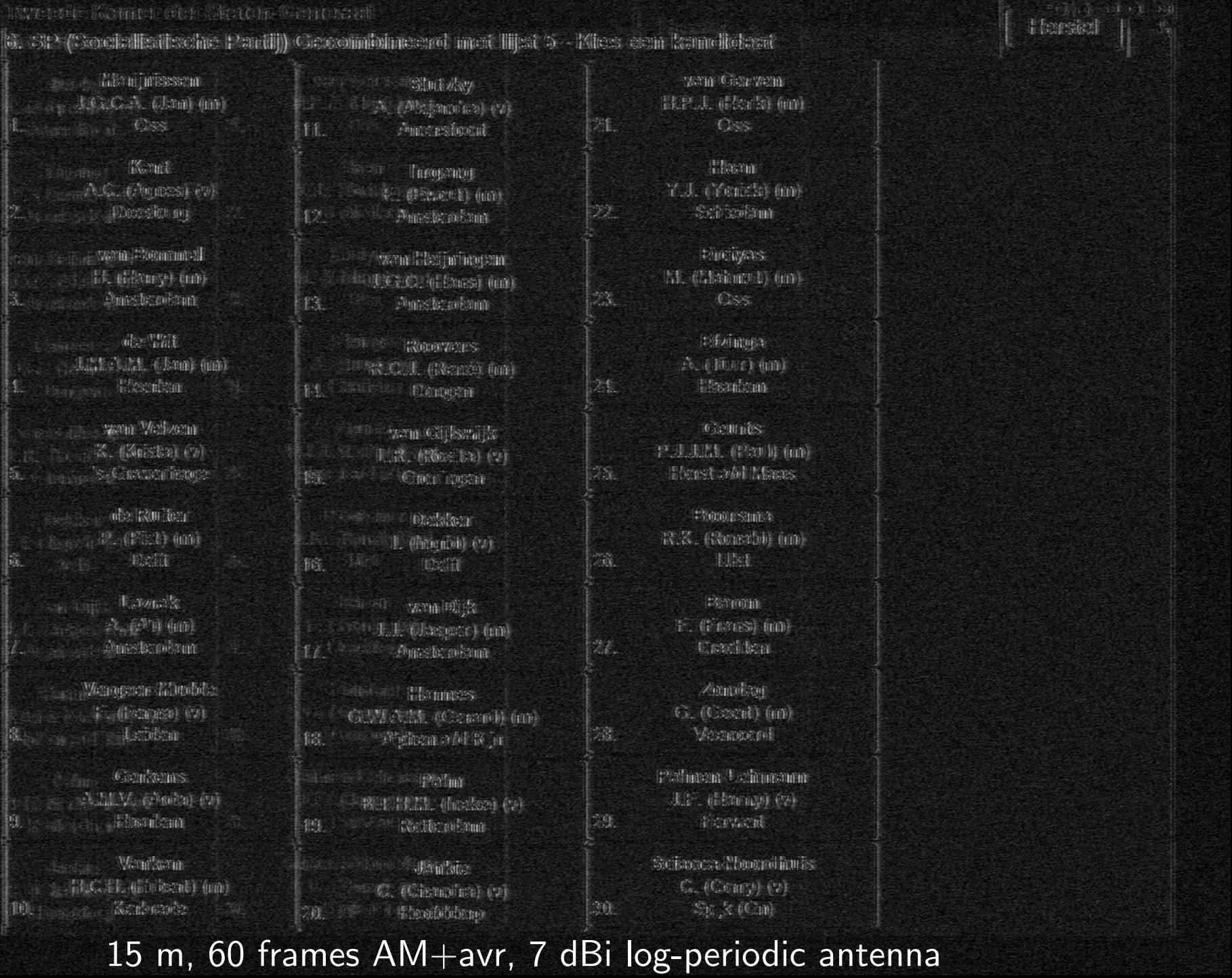
29. Palmen-Lehmann
J.F. (Hanny) (v)
Ferwert

Akkoord

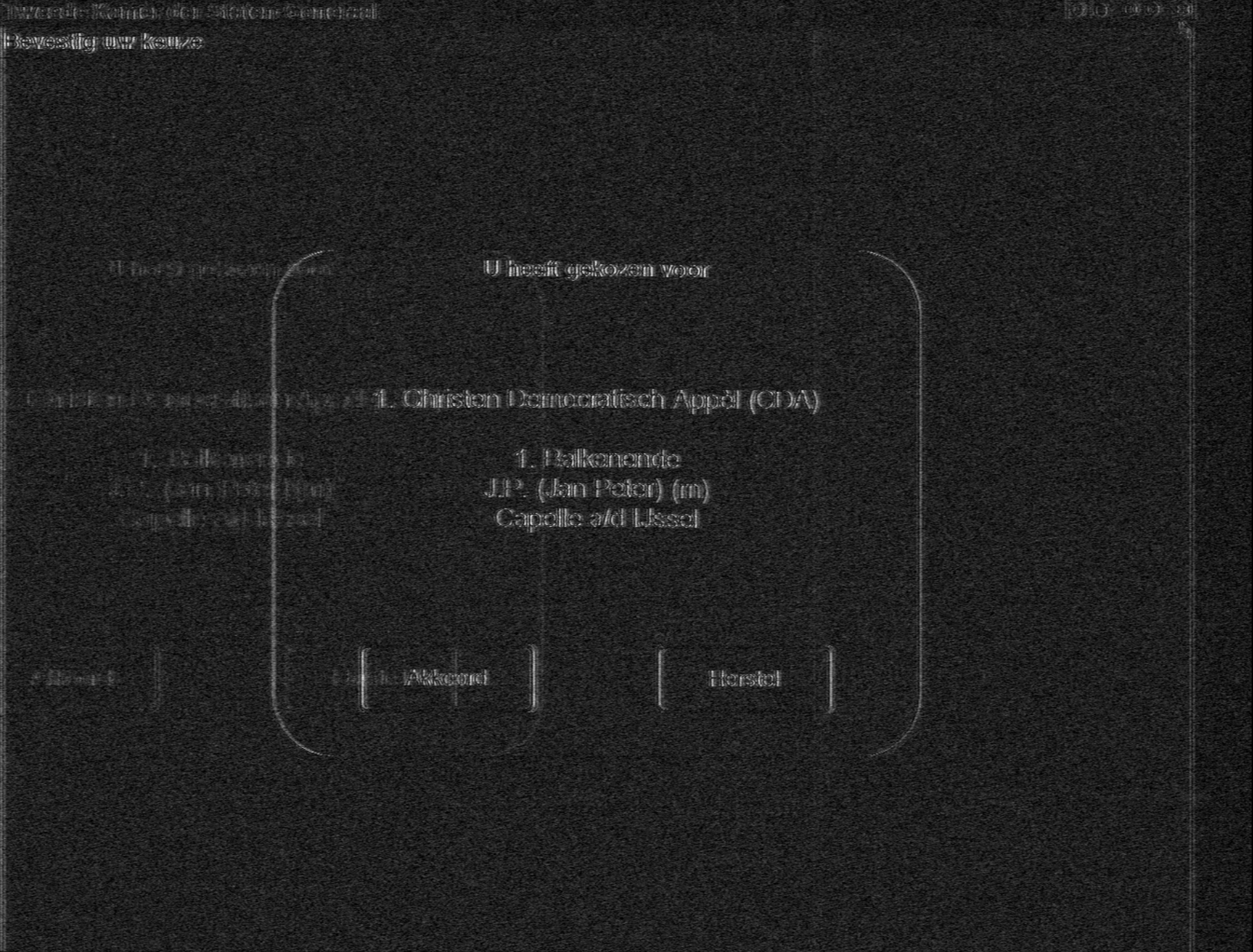
Herstel



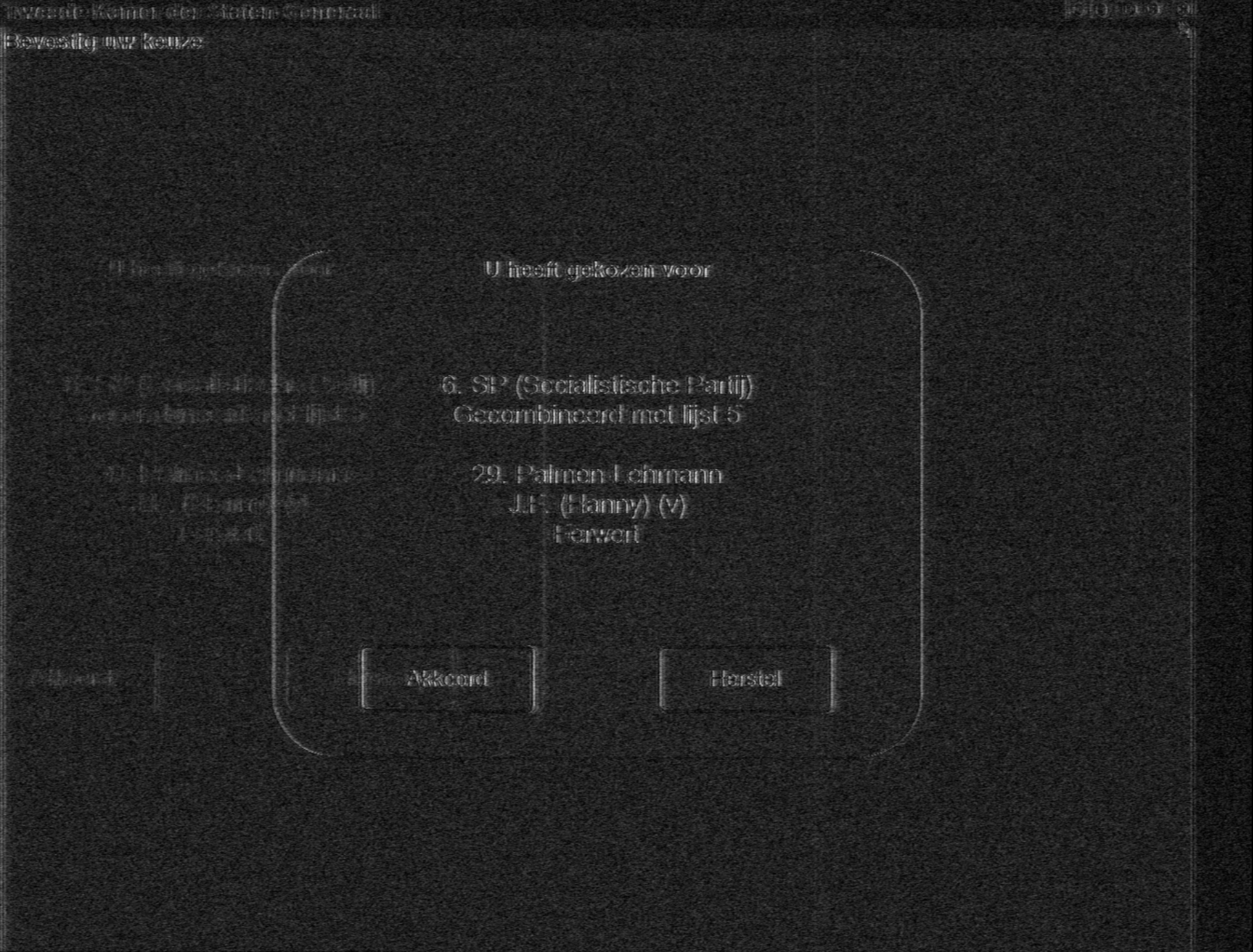
15 m, 60 frames AM+avr, 7 dBi log-periodic antenna



15 m, 60 frames AM+avr, 7 dBi log-periodic antenna



15 m, 60 frames AM+avr, 7 dBi log-periodic antenna



15 m, 60 frames AM+avr, 7 dBi log-periodic antenna

Simulating reception at larger distances

What if your corridor isn't long enough for measuring at $d = 40$ metres?

1. Record IQ signal $V_0(t)$ at antenna distance d_0 with antenna gain G_0
2. Record IQ noise $N(t)$ with same setup but target device switched off
3. Render IQ signal waveform

$$V(t) = 10^{\frac{G-G_0}{20\ \text{dB}}} \cdot V_0(t) \cdot \frac{d_0}{d} + N(t) \cdot \left(1 - \frac{d_0}{d}\right)$$

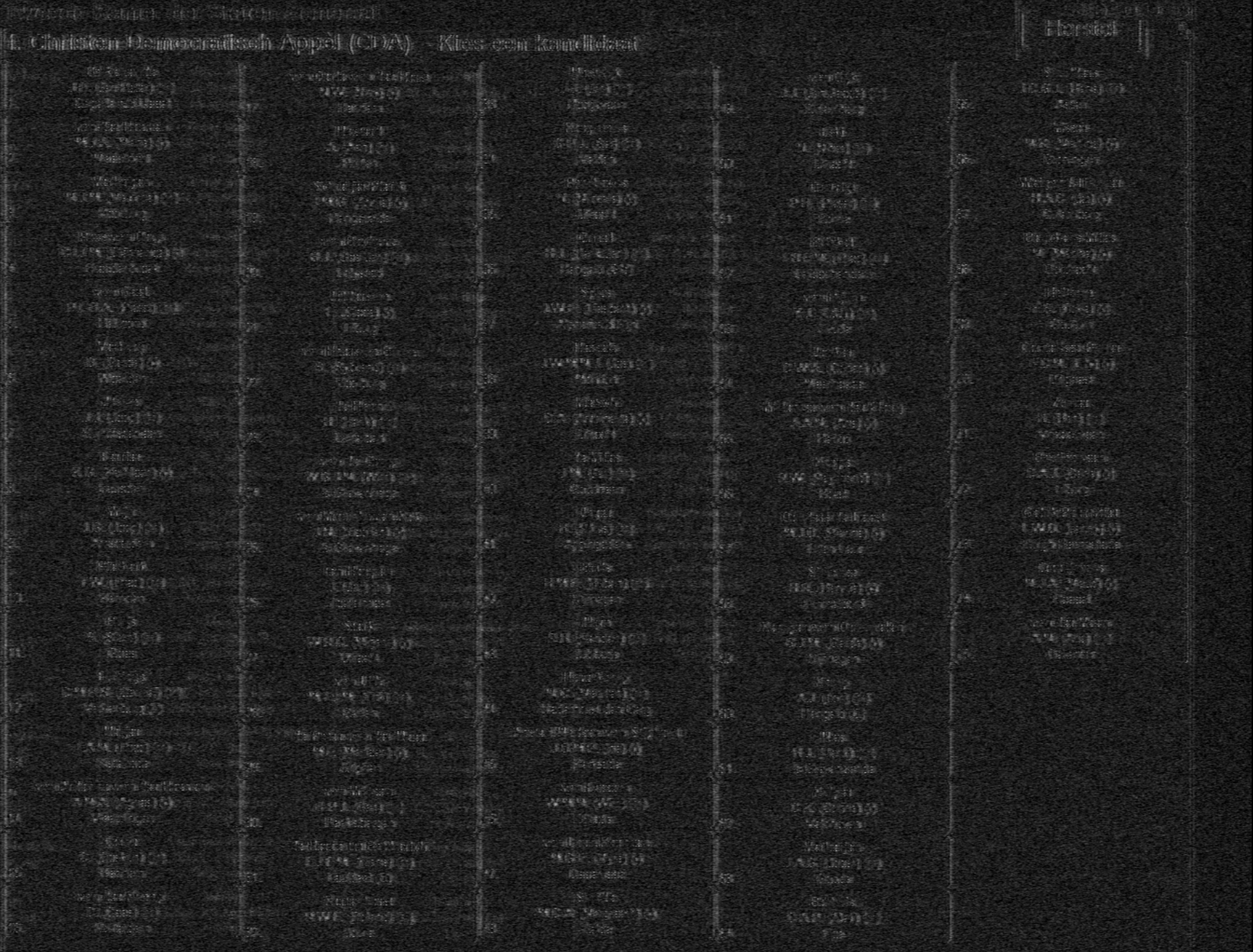
for simulated antenna distance $d > d_0$ and gain G

Make sure d_0 places the antenna well into the far-field of the emissions (Fraunhofer distance $d \gg \frac{2D^2}{\lambda}$, or simply $d > 2\lambda$, for wavelength λ and antenna/device diameter D).

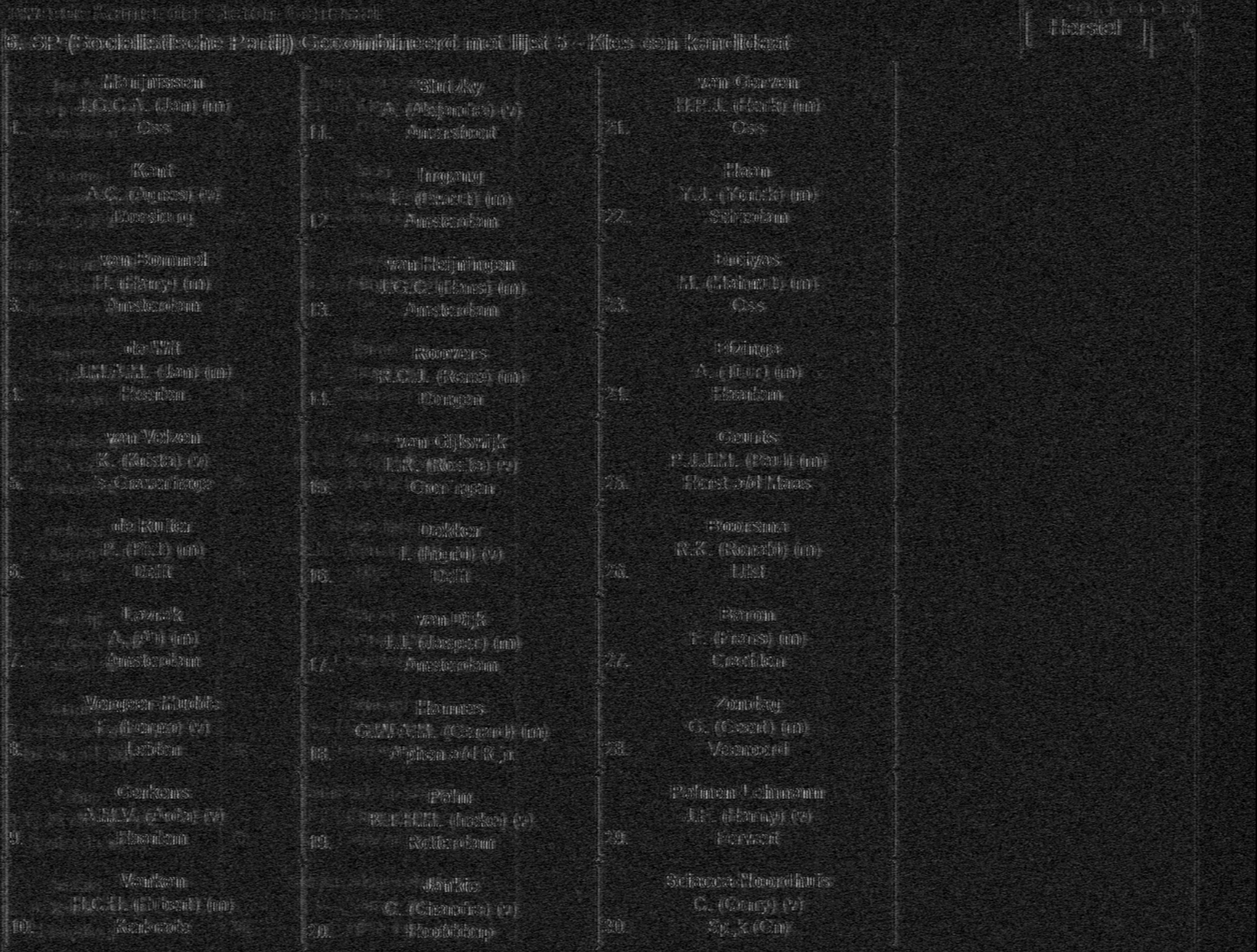
Beware that building corridors can act more like waveguides than just like free space (i.e., signal amplitude drops slower than $1/d$).



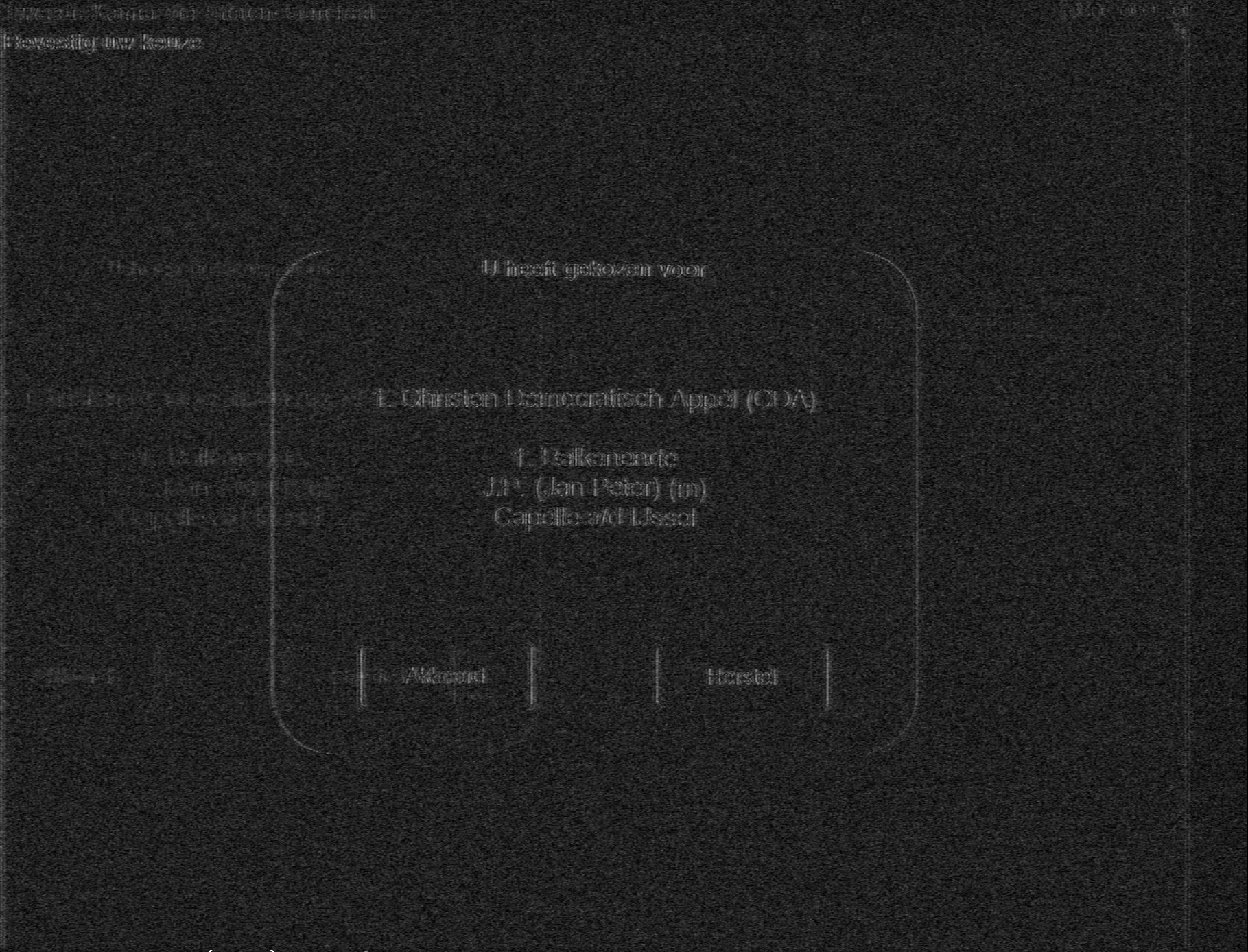
$d_0 = 15$ m, $G_0 = 7$ dBi



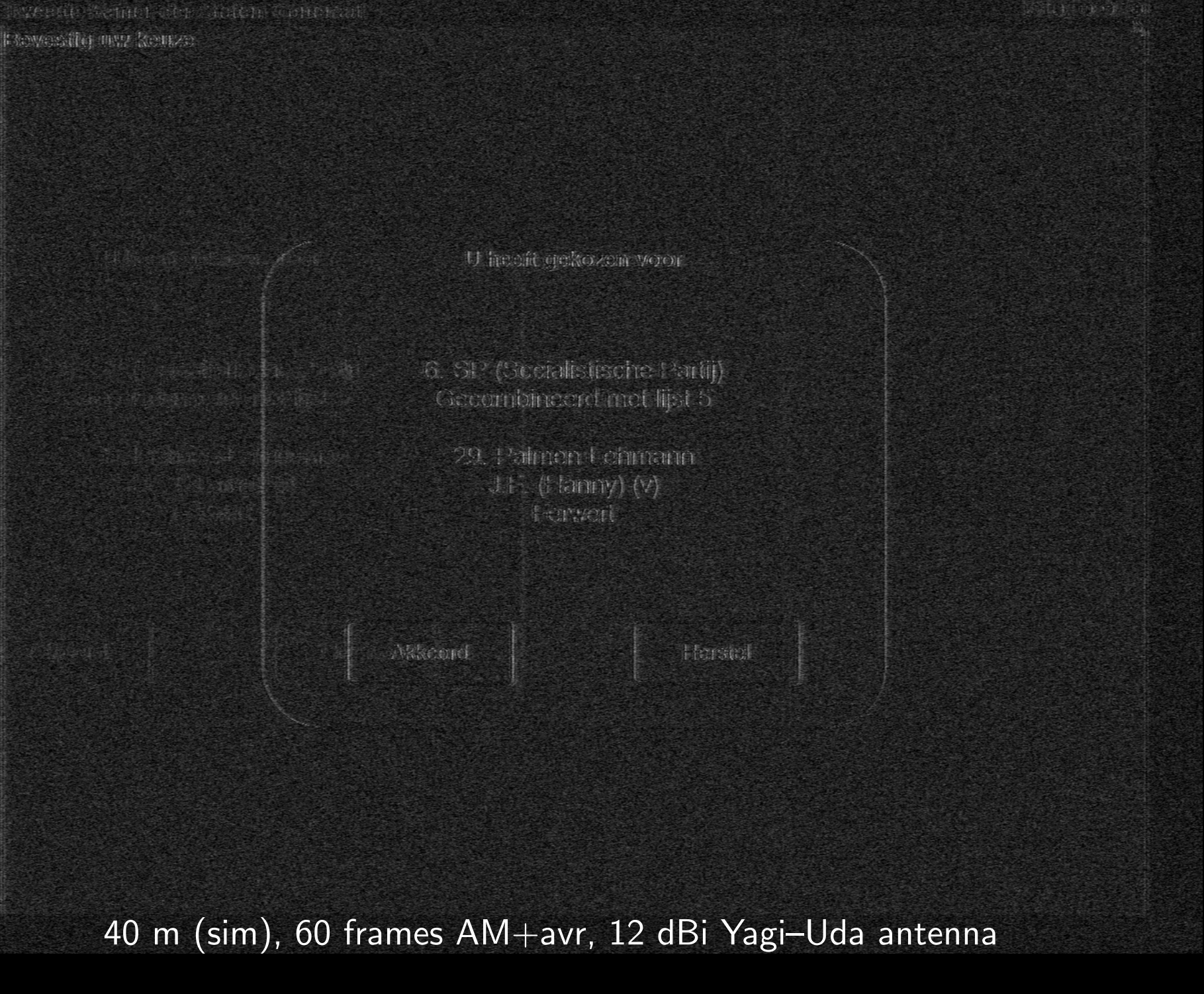
40 m (sim), 60 frames AM+avr, 12 dBi Yagi–Uda antenna



40 m (sim), 60 frames AM+avr, 12 dBi Yagi–Uda antenna



40 m (sim), 60 frames AM+avr, 12 dBi Yagi–Uda antenna



40 m (sim), 60 frames AM+avr, 12 dBi Yagi–Uda antenna

"It is remarkable nobody appears to have ever tested for any spurious emissions, or thought to include specifications regarding compromising emanations in the legal requirements. It would seem obvious that new versions of regulations regarding voting computers specify a level of shielding that prevents any such problems."

— Rop Gonggrijp, Willem-Jan Hengeveld, et al.

Three approaches

1. Limit curves
   - RFI standards obviously not suitable for information security
   - Simply use existing military TEMPEST standards (NATO SDIP-27 Level A/B/C)?
   - Suitable? What do they protect against? Zoning?
   - Confidential specification (and secret rationale) for public election infrastructure?
   - Independent verifiability?
2. Semantic security
   - Agree on adversary capabilities and rules of an evaluation game
3. Guidance for system designers
   - Practical lists of attacks to consider and pitfalls to avoid

Earlier attempts to define limit curves

TEMPEST

specifications and test methods

for e-voting machines

DRAFT

Version 1.4

2008-05-09

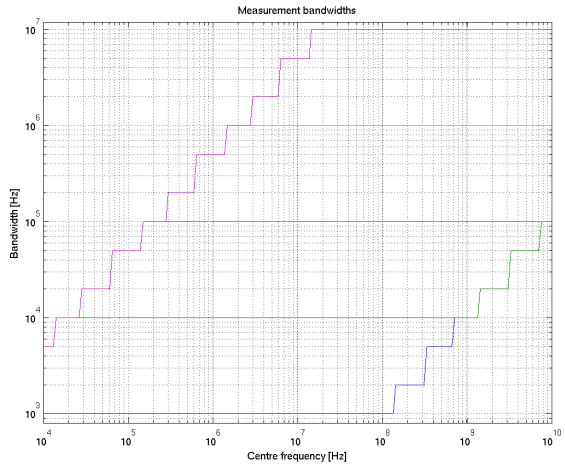


Figure 1

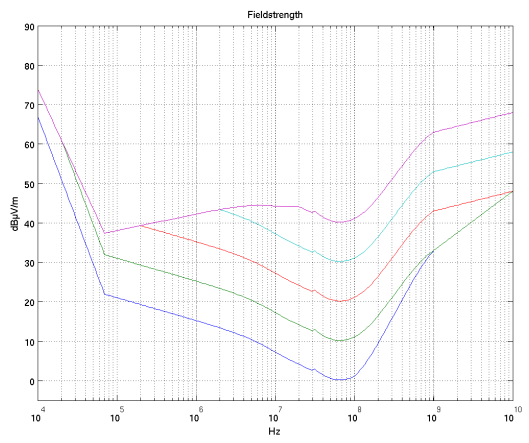


Figure 2

Voting is an unusual application

Very low bitrate signal:

- Say voter spends 4 seconds looking at 1 out of 16 party lists (or 4 seconds at the confirmation of 1 out of 16 candidates).
- Having ≈ 4 seconds to learn a ≈ 4 bit signal equates recovering

$$\approx 1 \text{ bit/s}$$

Can a set of spectrum-analyzer limit curves prevent a $C = 1$ bit/s signal within the $B = 50$ MHz (or larger) receiver band of an SDR?

Shannon–Hartley theorem suggests the limit curves would need to keep

$$S/N \ll 2^{C/B} - 1 = 1.4 \times 10^{-8} = -79 \text{ dB!}$$

Limit curves verifiable with **spectrum analysers** mainly able to avoid readability of unknown serial data. But in the case of voting, the small set of messages (candidate names) is already known a priori.

Cross-correlators with **integration times** of around 1 s may be needed instead for very low bitrates in high bandwidths.

Proposed specifications for the Dutch ballot printer

Bijlage:
Methode voor het bepalen van effectiviteit van maatregelen tegen compromitterende straling

Ballot printer – performance of eavesdropping protection –radio-frequency emissions

1 Introduction and scope

This specification aims to define the level of eavesdropping protection expected from a ballot printer. A ballot printer is a device (typically a desktop unit) that can be configured with a ballot configuration file *C*. This file defines and names the n choices $\{c_1, c_2, \ldots, c_n\}$ that a voter can make during the election process. A typical configuration file *C* may contain a list of political parties and/or candidates, or a list of options for a referendum, along with associated names, logos, portrait photographs, or accompanying descriptive text that the ballot printer displays to assist the voter in making their choice, or prints onto the resulting ballot paper. A voter can use the ballot printer to make one choice *X* out of the available *n* options defined by the configuration file, and the device then records that choice by printing out a ballot paper that the voter can fold and take away to the ballot box. The choice made by the voter has to remain confidential, and must not become known to anyone else until the ballot box is opened and the ballot paper is unfolded during the counting process, at which point the ballot paper should no longer be linkable to the voter.

One security concern in the design of such a ballot printer is that electromagnetic signals that are unintentionally emitted by its circuitry can give away the voter's choice to a nearby eavesdropper with suitable antennas, radio receiver and signal-processing equipment.[1] Whether such an eavesdropping attack is feasible or not depends on a number of factors, such as at what distance can the eavesdropper use what type of antenna, what is the background noise level in the environment, and how detailed and accurate must the eavesdropped information about the voter's choice be to count as a successful attack. It is not practical to shield devices completely against every imaginable form of an electromagnetic eavesdropping attack, for a number of reasons. While electric fields can be shielded relatively easily using a metallic enclosure (Faraday cage), shielding magnetic fields is far more difficult. Very close to the device (in the *near field*), magnetic fields can be the dominant form of emissions, but will also drop off rapidly with increasing distance. It may not be difficult to demonstrate a successful eavesdropping attack that estimates the choice of the voter with slightly better chances than random guessing, using large antennas placed centimetres from the surface of the device, with both the device and the antenna located in a shielded chamber that eliminates environmental background noise.

[1] Acoustic or optical eavesdropping attacks (using microphones, or sensors for diffusely reflected light) are also a potential threat, but outside the scope of this document. However, Section 5 offers some related informal notes.

Bijlage:
Richtlijnen ter voorkoming van compromitterende straling

Ballot printer – protection against eavesdropping attacks – guidance for system designers

1 Background

In 2007, the Dutch government reviewed the security and use of electronic voting machines in elections, after the campaigning group "Wij vertrouwen stemcomputers niet" had published a report [1] demonstrating a number of attacks against such devices.

One of these demonstrations exploited electro-magnetic radiation that was unintentionally generated by the electronics inside a voting machine that was withdrawn in 2007, which accidentally revealed information about what political party the user is choosing. This information could be exploited by anyone with a suitable radio receiver tuned to the right frequency, as had been demonstrated at 25 m distance. The particular problem exploited there was that the device's software continuously updated a liquid-crystal display with the currently displayed text, and due to the particular encoding required for that text, the repetition time of that software loop depended on the number of (non-ASCII) characters with diacritical marks displayed. One of the political parties (Christen-Democratisch Appèl, CDA) listed on the electronic ballot sheet has an "è" character in its name, and the display of that character reduced the rate at which the software loop executed. That rate was audible as a buzzing sound with an AM radio, on many tuning frequencies throughout the HF and VHF radio spectrum, and that buzz lowered its frequency whenever the CDA party name was displayed. A demonstration video [2] released by the campaigning group featured a "CDA detector", a user-friendly improvised detector device that indicated visually whether a nearby voting machine was currently displaying a diacritical character or not.

Subsequent testing by a government laboratory [3] revealed that a second type of voting machine that was withdrawn in 2006 also was vulnerable to radio-frequency eavesdropping, revealing much more useful information, at even larger distances. This voting machine featured an integrated 1280×1024-pixel flat-panel video display that was refreshed at 60 Hz by an internal analogue VGA-cable video interface. With a suitable wide-band receiver tuned to multiples of the pixel frequency (108 MHz), e.g. at 432 MHz, and the help of raster-display software, a remarkably clear copy of the video image could be reconstructed tens of metres away. Software-defined radio equipment that can be programmed to visualise such compromising video signals is now widely available to hobbyists for less than 800 euros. A closer investigation by the author at the time revealed that the graphics controller used on the embedded PC main board found in the second type voting machine was the source of these emissions. Its three (red, green, blue) digital-to-analogue converter circuits together emitted the sum of the red, green and blue voltage generated for the VGA output as an amplitude-

https://www.tweedekamer.nl/kamerstukken/detail?id=2016D17983&did=2016D17983
https://www.tweedekamer.nl/kamerstukken/detail?id=2016D17984&did=2016D17984

Semantic security

Idea: specify eavesdropping security as a game between a

- *challenger* (voting machine designer) and
- *adversary* (eavesdropping demonstration designer)

Similar to cryptographic ciphertext-indistinguishability definitions (Goldwasser/Micali IND-CPA)

Voting machine (e.g., ballot printer) has a configuration file C enumerating n choices for the voter: $\{c_1, \ldots, c_n\}$.

C may contain a list of political parties and/or candidates, or a list of options for a referendum, along with associated names, logos, portrait photographs, or accompanying descriptive text that the device displays to assist the voter in making their choice, or prints onto the resulting ballot paper.

Game: setup

- Choose two devices at random out of a manufacturing batch
- Give adversary access to one of these, for laboratory tests and reverse engineering.
- The other sample device remains intact and will be used as the target of evaluation (TOE) in the following experiment.
- The adversary provides a valid configuration file C, which a referee loads into the TOE. The file must pass all the acceptance tests implemented by the device.
- Then repeat the following steps k times:

Game: challenge rounds

1. Prepare the TOE for the next vote.
2. The adversary sets up or adjusts their eavesdropping equipment, within the constraints set out in the next section.
3. The adversary chooses two of the ballot choices available in that configuration file, c^0 and c^1, and hands these to the challenger.
4. The challenger picks a random bit b (e.g. by tossing a coin) and instructs a neutral voter to use the TOE normally to vote for c^b
5. The adversary can see when the voter starts and finishes using the TOE. The adversary observes the TOE through their eavesdropping equipment while the voter uses the device.
6. The adversary examines data received and then announces their best guess b' for the value of the secret bit b chosen by the challenger.
7. The challenger/voter now reveal their secret bit b. If $b = b'$, then the adversary has guessed the vote correctly and won this round.

The TOE has failed the test if the adversary can demonstrate that they can guess the random bit b correctly $w \geq 45$ times in $k = 60$ rounds.

Eavesdropping setup

The eavesdropper's equipment must comply with these restrictions:

R1 At least 8 metres horizontal distance between the outer surfaces of the TOE and any eavesdropping equipment

R2 All radio antennas used (excluding tripod/mast legs used for positioning) must together fit into a cuboid of width 1.0 m, height 0.9 m and length 1.2 m

R3 May include voltage-probe and current-clamp access to the power-supply cable of the TOE (again at 8 m distance)

Alternative eavesdropping setup

Alternatively, the adversary may choose the following conditions for a very compact eavesdropping system:

C1 At least 4 metres horizontal distance between the outer surfaces of the TOE and any eavesdropping equipment

C2 All equipment (antennas, receivers, processors) fits comfortably inside a typical 20-litre backpack (such that the backpack remains externally indistinguishable from one filled with books or clothes)

C3 Weighs not more than 8 kg

C4 Does not require any access to a power line (or other external wired connection)

C5 Includes a power supply (battery) for three hours

C6 Does not require any on-site adjustment other than crude one-off placement and orientation

Rationale

- Adversary has to learn only 1 bit of information (like CDA detector)
- Adversary has control over config file, can pick party/candidate names/logos/portraits that are particularly easy to distinguish (like non-ASCII characters were with the Nedap machine)
- Adversary can calibrate attack on a type-identical model (profiled template attack)
- On-site recalibration on TOE device is possible, but will cost rounds
- 8-meter setting aims to represent directional antenna feasible in adjacent room or vehicle parked near outside wall.
- 4-meter setting aims to represent covert non-directional antenna in same room

Implementation guidance: video interfaces

- avoid analog or asymmetric interfaces like VGA
- avoid conversion between video interfaces and modes
- avoid digital interfaces with simple line encodings, like FPD-Link
- on HDMI or DisplayPort try to enable HDCP
- DisplayPort can be *much* more challenging to eavesdrop than TMDS (bitrate independent of video mode, 16-bit LFSR scrambler resets every 512 lines, long periodicity and 1-byte uncertainty in byte/pixel alignment hinder periodic averaging, AM/FM demodulation useless, correlation attacks computationally very expensive, etc.)
- enable FM modulation of clock signals where supported (e.g., DisplayPort option)
- in DisplayPort chose odd total height of video mode
- consider randomizing less-significant bits in data-independent way
- consider randomizing display layout (e.g., permuted lists)

Implementation guidance: other considerations

- avoid busy-wait loops (= narrowband transmitters)
- capacitive touchscreen incompatible with transparent shielding
- the usual EMC guidance
  (conductive shielding, filters, avoid ground-return loops, avoid common-mode currents)
- disable wireless transmitters during the vote (while the device handles confidential data)
- consider optical leaks (e.g. overall display brightness)
- consider acoustic leaks (e.g. from headphones for visually impaired users)
- consider power-line emissions

Concluding notes

- at least one civilian application with a TEMPEST requirement
- ballot-printer + vote counter ultimately was dropped, return to paper and pencil
- a simple vulnerability demonstration (even if very constrained) can shatter public confidence in a product or concept
- constitutional requirements for secrecy of ballot nonnegotiable
- in some regions of the world real risks of bribery of, or sanctions against, voters