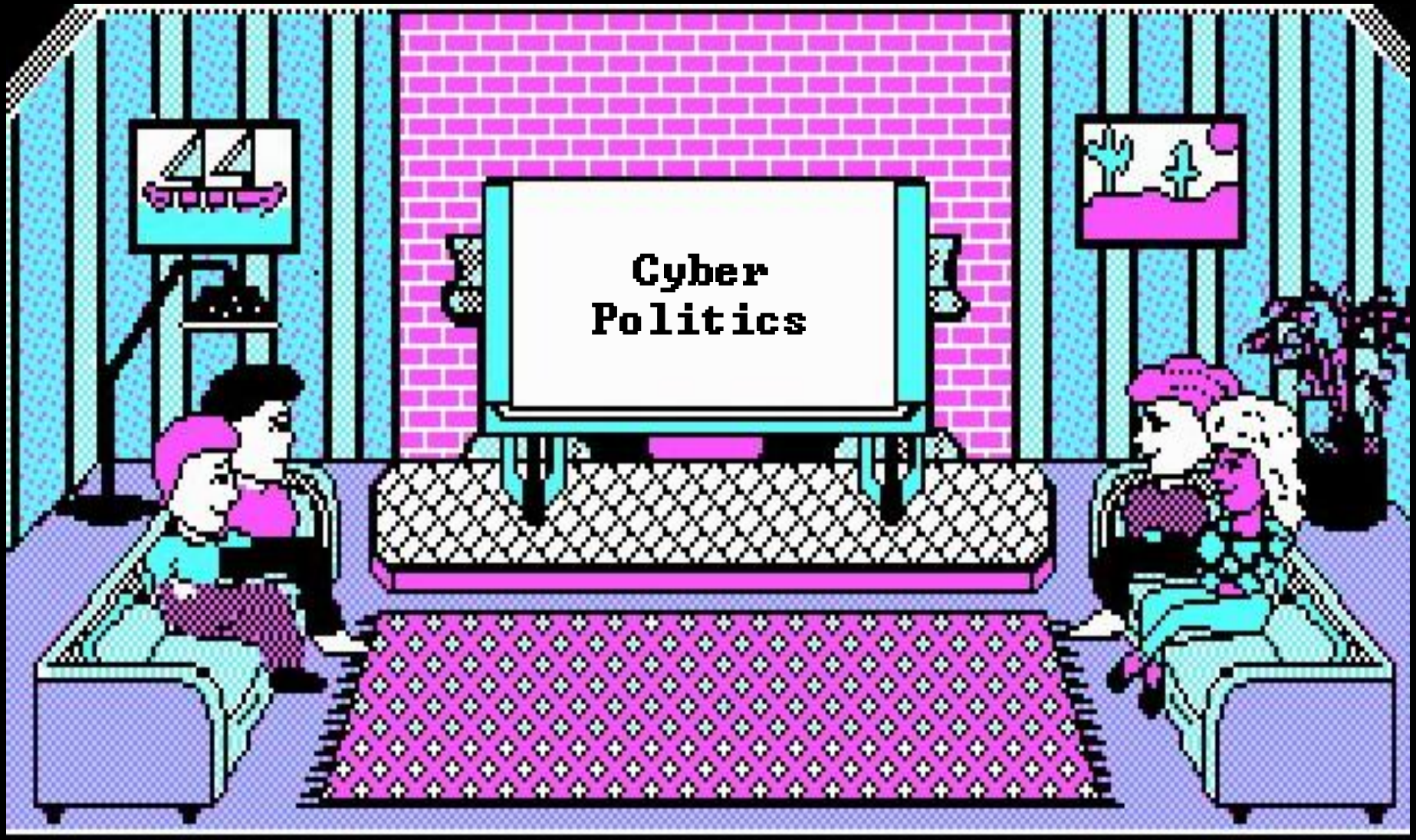
H2HC

TEST DRIVE

CTRL - (J)OYSTICK OR CTRL - (K)EYNOTE

Politische Weltkunde
beim Oberpaketsturmfuehrer

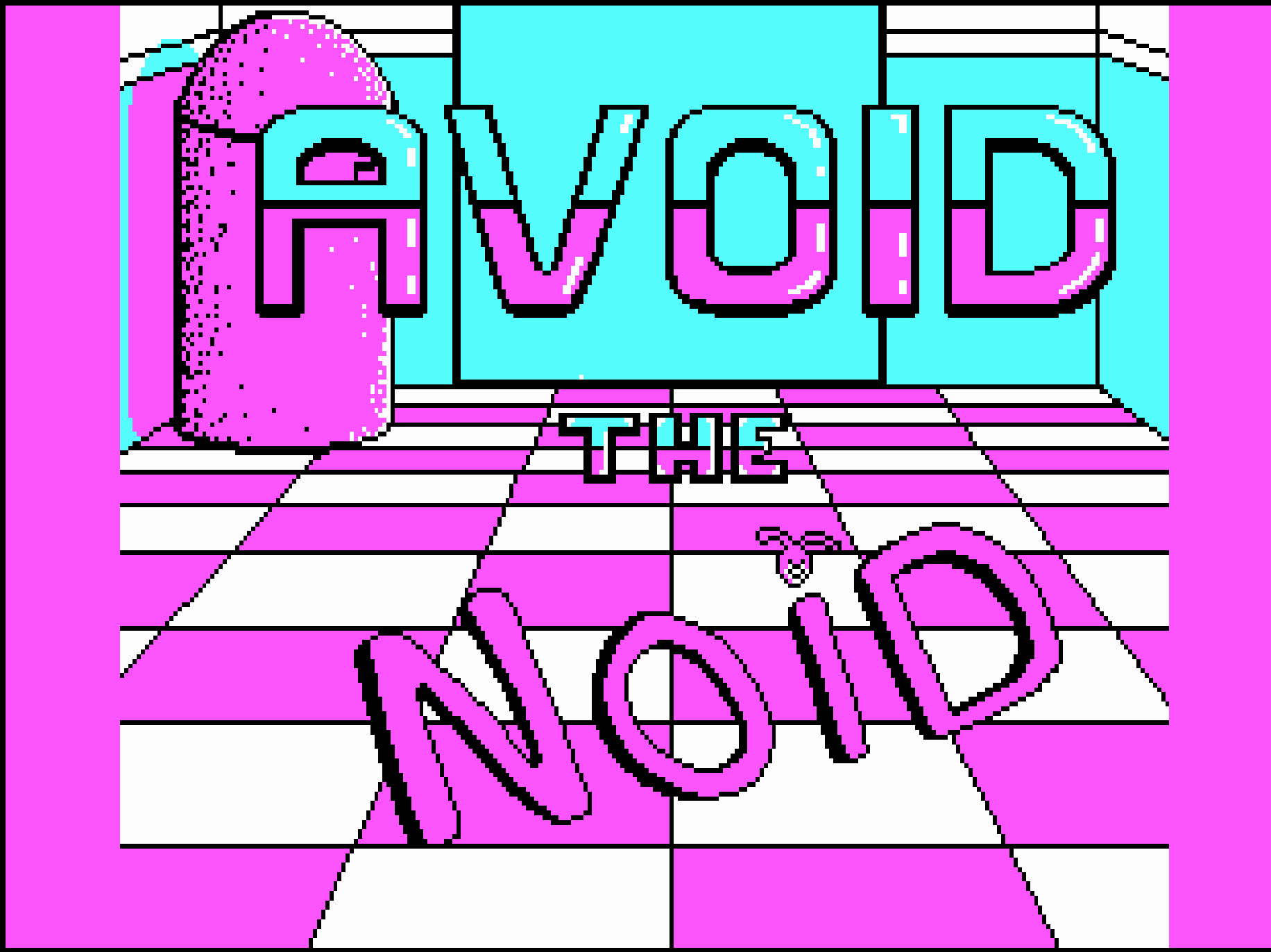


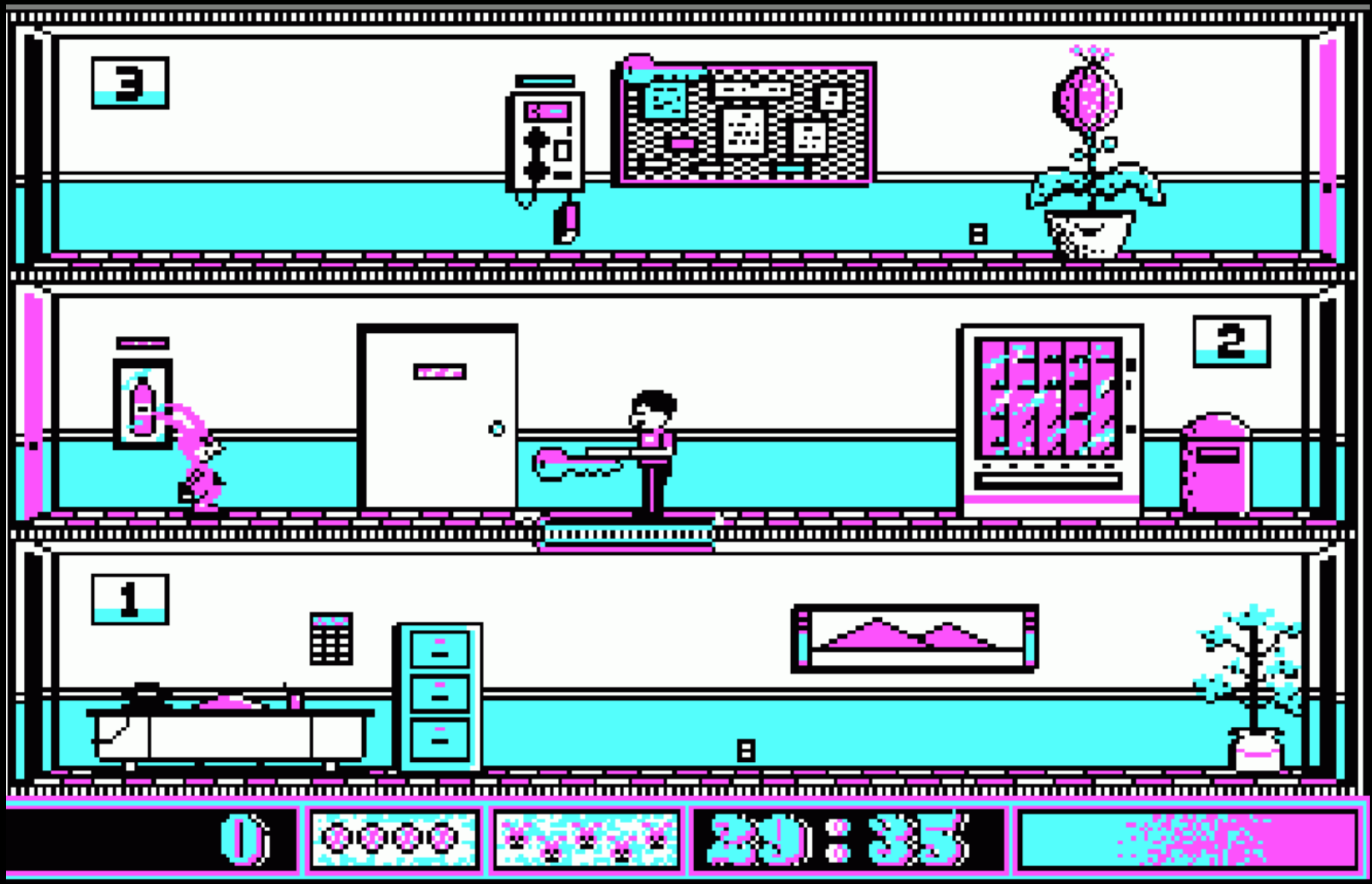
WELCOME TO
WIN, LOSE OR DRAW!

Fuck Politics!
I`m 31337!

- "Hackers don't care about politics!"
  - And Full Disclosure is not a political debate exactly how?
- "I already vote Pirate Party!"
  - If that's also how often you update your systems, the argument is valid.
- "They are all corrupt anyway."
  - And that's why you let them run your life?
- "Can we talk about exploits already?"
  - We actually do.
- "Politics is for old fat farts"
  - Correct, that's why they put me up here.


CONGRATULATIONS!
You lose!


AVOID
THE
VOID



Reality is: Where the pizza guy comes from.

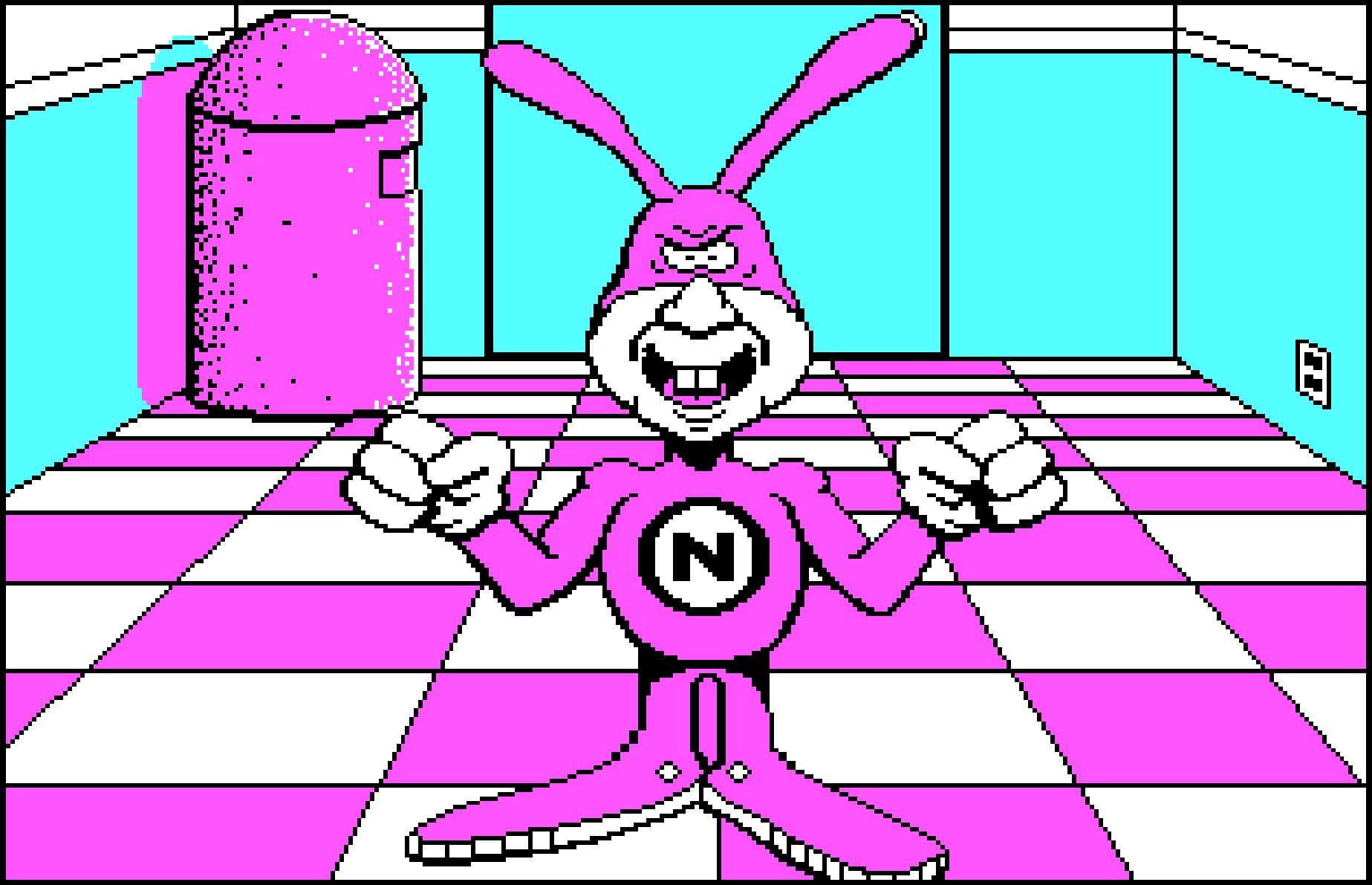
Cyber Politics

- From the Greek word Politikos: "of, for, or relating to citizens"
  - Citizens, that's all of us
    - Minus the 12 million the UNHCR counts
- "There are no true friends in politics." – Marcus Tullius Cicero
  - This from the mouth of the prophet, the archetype of the career politician
  - Friendship is largely about yielding
    - Politics seem to be awfully important to people – look at how rare yielding is
- Cyber: William Ford Gibson (*1948)

Not A New Problem

- To what extent may human interrelations be governed by art or skill?
- What is the nature of the expertise required in politics?
- Does political philosophy ever achieve the status of knowledge?

Plato



Avoid the Noise(bridge)

THIS IS NOT HACKTIVISM!

This is civilization.

You never know what it is good for

- You ...
  - ...helped create something secure and usable
  - ...didn't receive financial benefits
  - ...watch while only a few politicians benefit from it
    - Exactly one, in my case ;)
- Have you made a mistake?
  - Or have you created political options?
    - Options turn into policy quickly
- Spender and the PaX Team are the Johannes Keplers of computer security
  - Others like to portray themselves as Galileo Galilei, without the work part

Don't let anyone tell you what to do

- Most people that lecture you on ethics don't follow those themselves
  - Digital human rights activists who also head companies selling to military or criminal mobs
  - People bashing Microsoft while sitting at their campus, getting paid very well
  - People writing spy software for oppressive governments while considering themselves to be left wing activists
- There are many aspects to consider
  - Other people's opinion isn't one
- This is Real Life. Welcome.
  - Please do people a favor and shut the fuck up, until you lived up to your own rhetoric.

[S]ell or [N]ot?

- Is selling exploits like selling weapons?
- Weapon, (n): Tool to damage another living being's physical and mental capacity to act, injure it or kill it.
  - Do you think it should be illegal?
  - What about regulating use?
  - Do you think you can control what your exploit is used for? Do you care?
  - Is it better or worse than leaking docs to Wikileaks?
- "Do whatever you want. Trust your guts, your humanly feelings, your very limited knowledge. This is best effort."
  — Julio Auto

Bad Religion!

- Having worked for "the bad people" does not get you into hacker hell
  - Unless you fucked it up, of course
    - Let's be honest, being the author of Stuxnet makes you cool, FinFisher not so much
- Running 512 Tor nodes doesn't give you absolution from your sins
  - Especially not if you put them on EC2
  - Unless they are exit nodes and you still have all the PCAPs ;)
    - United States Naval Research Laboratory?
    - Bundesstelle fuer Fernmeldestatistik!
- Don't you have work to do?
  - While some are busy playing the ethics charade, we still cannot build or buy secure computers.

Worst Approach Ever

- Wide audience publishing
  - Always criticizing, buddies excluded
- Not getting involved
  - A showcase in cowardice
  - The best strategy to preach water and drink wine (or get paid, if you fail at drinking)
- Demonstrating an attitude of considering oneself better and above the society
  - Yes, "society" are the idiots out there
    - The same idiots that bring your pizza

RICK DANGEROUS II

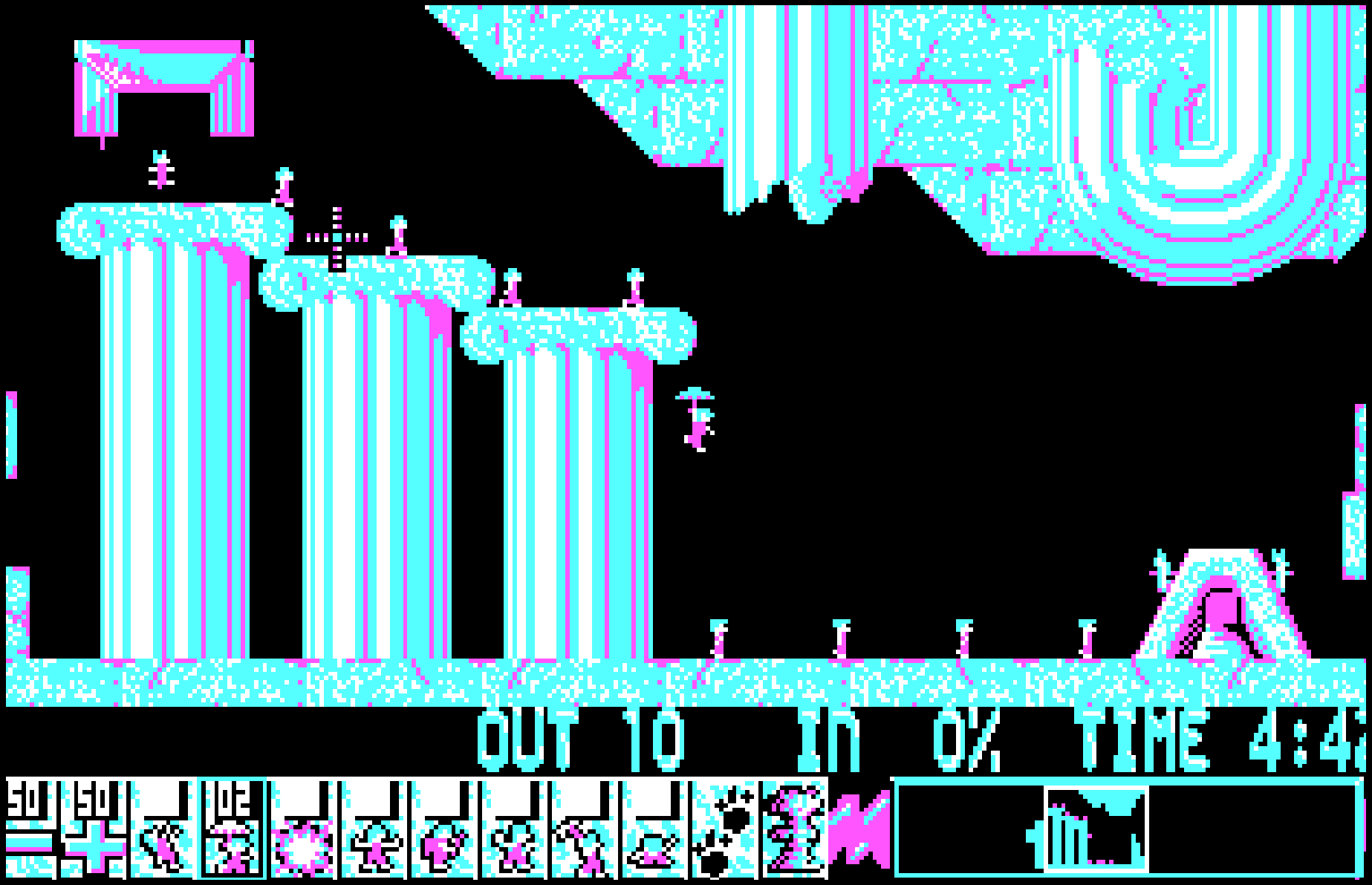
You think that's you?

```
10 DIMENSION INS(100)
20C
30C ------------------------------------------
40C INS IS THE ARRAY INTO WHICH INSTRUCTIONS ARE
50C BY THE PENETRATOR
50C ------------------------------------------
70C
80 DATA INS(1)/0635004/
90 DATA INS(2)/02755004/
100C
110C ------------------------------------------
120C THE VALUE OF IBRK IS EQUIVALENT TO TRA 0,3
130C ------------------------------------------
140C
150 DATA IBRK/0710013/
160C
170C ------------------------------------------
180C SETS UP THE RETURN
190C ------------------------------------------
200C
210 ASSIGN 200 TO N1
220C
230C ------------------------------------------
240C PLACES THE RETURN IN THE ARRAY
250C ------------------------------------------
260C
270 INS(3)=N1
280C
290C ------------------------------------------
300C ASSIGNS VALUE 1 TO INTEGER VARIABLE N2
310C------------------------------------------
320C
330 N2=1
340C
350C ------------------------------------------
360C NEXT STATEMENT CAUSES X3 TO BE LOADED WITH
370C OF THE FIRST WORD OF THE ARRAY INS
380C ------------------------------------------
390C
400 INS(N2)=INS(1)
410C
420C ------------------------------------------
430C COMPILES AS A DIRECT TRANSFER TO THE INTEGE
440C ------------------------------------------
450C
460 GO TO IBRK
470C
480C ------------------------------------------
490C CONTROL RETURNS HERE FROM CODE IN INS
500C ------------------------------------------
510C
520 200 PRINT 201,INS(4)
530 201 FORMAT(1X,012)
540 STOP
550 END
```

```
20 DIMENSION IFIL(33)
30 DIMENSION ICHR(64)
40 DIMENSION IDUM(13),JDUM(24)
50 DIMENSION IBIG(24)
60 ASCII ICHR,JDUM
70 DATA ICHR/0060000000000,0061000000000,0062000000000,
80& 0063000000000,0064000000000,0065000000000,0066000000000
90& 0067000000000,0070000000000,0071000000000,0043000000000
100& 0043000000000,
110& 0100000000000,0072000000000,0076000000000,0077000000000
120& 0040000000000,0101000000000,0102000000000,0103000000000
130& 0104000000000,0105000000000,0106000000000,0107000000000
140& 0110000000000,0111000000000,0046000000000,0056000000000
150& 0135000000000,0050000000000,0074000000000,0134000000000
160& 0136000000000,0112000000000,0113000000000,0114000000000
170& 0115000000000,0116000000000,0117000000000,0120000000000
180& 0121000000000,0122000000000,0055000000000,0044000000000
190& 0052000000000,0051000000000,0073000000000,0047000000000
200& 0053000000000,0057000000000,0123000000000,0124000000000
210& 0125000000000,0126000000000,0127000000000,0130000000000
220& 0131000000000,0132000000000,0137000000000,0054000000000
230& 0045000000000,0075000000000,0042000000000,0041000000000
240 DATA IFIL/036002000,0001356,02001411,0,0,0,0,
250& 0001361000000,0001372001363,0001364000000,0,0,
260& 0740000000000,0,02000002,0510102010000,0000220202020
270& 0760000000000,0777777777777,0510102010000,
280& 0000220202020,0202020202020,0202020202020,0777777777
290& 0510102010000,0000220202020,0202020202020,0202020202
300& 0102122113062,0040040040040,0040040040040,0040040040
310& 0777777777777/
320 KKK=2
330 LLL=2
340 DATA IP3/01373/
350 DATA IP4/01376000000/
360 DATA IP5/01414001400/
370 DATA IP6/01401000000/
380 DATA IBRK/0710013/
390 DATA IP77/01700000000000/
400 DATA IP1/02001433/
410 DATA INS(1)/0635004/
420 DATA INS(2)/02755004/
422 DATA IP98/00600000000000/
430 DATA IP99/051010303000301/
440 GO TO(600,601),KKK
450 600 CONTINUE
460 ASSIGN 677 TO N1
470 INS(3)=N1
480 N2=1
490 INS(N2)=INS(1)
500 GO TO IBRK
510 677 PRINT 678,INS(4)
520 678 FORMAT(1X,012)
530 GO TO 602
540 601 CONTINUE
550 DO 77 I=1,33
560 INS(I)=IFIL(I)
570 77 CONTINUE
580 INS(3)=IP1
590 INS(2)=IP3
600 INS(8)=IP4
```

```
630 INS(25)=0
640 INS(16)=IP99
650 INS(26)=0
660 INS(26)=0
670 101 FORMAT(1X,I4,1X,012)
680 66 CONTINUE
685 PRINT 101,INS(25),INS(25)
690 DO 79 I=34,500
700 INS(I)=0
710 79 CONTINUE
720 ASSIGN 200 TO N1
730 INS(4)=N1
740 N2=1
750 INS(N2)=INS(1)
760 GO TO IBRK
770 200 CONTINUE
780 GO TO(604,605),LLL
790 604 CONTINUE
800 DO 615 I=1,40
810 IF(INS(I)) 616,615,616
820 616 PRINT 101,I,INS(I)
830 615 CONTINUE
840 GO TO 602
850 605 CONTINUE
860 J=0
865 GO TO 714
870 715 CONTINUE
880 IF(INS(102+J) .NE. INS(105+J)) GO TO 805
882 IF(INS(102+J) .EQ. 0) GO TO 805
890 714 CONTINUE
900 IF(INS(102+J) .EQ. IP77) GO TO 716
910 INS(102)=INS(105+J)
920 INS(103)=INS(106+J)
930 INS(110)=INS(110+J)
940 INS(111)=INS(111+J)
950 5 FORMAT(1H ,3(012,1X))
960 ENCODE(IDUM,1)INS(102),INS(103),INS(110),INS(111)
970 1 FORMAT(4(012))
980 DECODE(IDUM,13)(IBIG(I),I=1,24)
990 13 FORMAT(48(02))
1000 DO 99 I=1,24
1010 IK=IBIG(I)+1
1020 JDUM(I)=ICHR(IK)
1030 99 CONTINUE
1040 PRINT 3,(JDUM(I),I=1,24)
1050 3 FORMAT(1H ,12(A1),1X,12(A1))
1060 713 J=J+12
1070 GO TO 715
1080 716 CONTINUE
1090 INS(25)=INS(25)+1
1100 GO TO 66
1120 805 J=J+1
1130 IF(J .GT. 500) GO TO 716
1140 IF(J+100 .GT. 500) GO TO 716
1150 IF(INS(100+J) .EQ. IP98) GO TO 807
1160 IF(INS(100+J) .EQ. IP77) GO TO 716
1170 GO TO 805
1180 807 CONTINUE
1190 GO TO 715
```


Kernel Memory Corruption Exploit in Fortran
James P. Anderson, US Air Force, 1972



That's more like it.

How About a Little Abstraction?

- [D]escribe or [P]rescribe, choose
  - Granularity of the choice is very high
- Publishing exploits is describing
  - It is supposedly also a proof by construction, but that's Sergey's problem
- Bug bounty programs are prescription
  - The vendor prescribes your hobby to you
- Sitting on > 50 0days for a single platform is a form of neutrality
  - Greetings to Germany, how Swiss of you ;)
- Madness? THIS IS HACKING!

DEFENSE, BABY!

It's ethical, included.

Look! NSA! How Evil!

Collective Reality Distortion

- "Google's mission is to organize the world's information and make it universally accessible and useful."
  - Where is the income from "information access" in Google's annual reports?
- "[Gen.] Alexander's strategy is the same as Google's: I need to get all of the data" – NSA source
  - "[...] an amount of information about 50 percent larger than what Google processes in [a single day]"
- Who holds the patent for MapReduce?
  - Notice something?

Like Lambs to the Slaughter

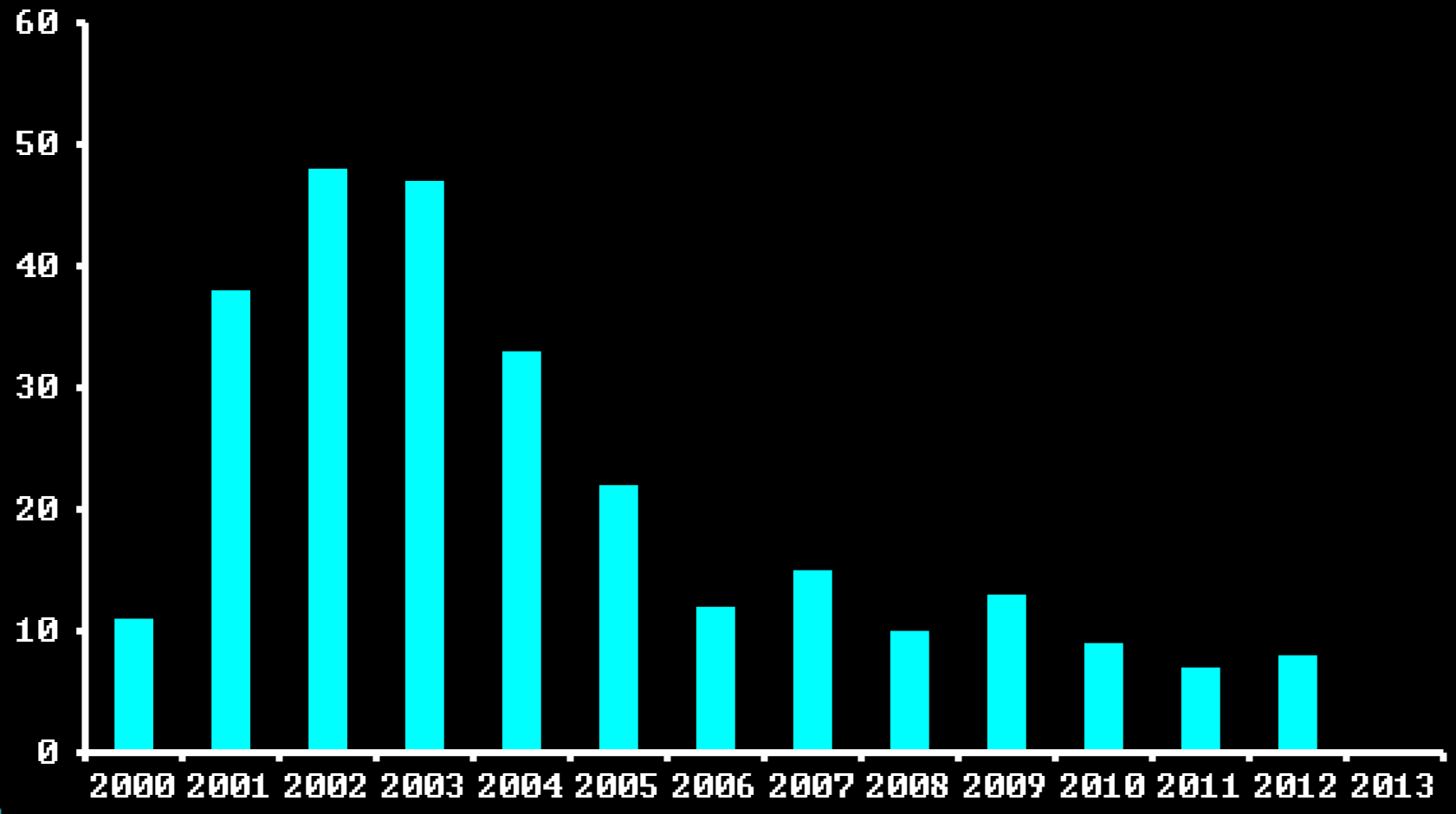
- "We do have a facebook page and a twitter account:
  https://twitter.com/h2hconference
  https://www.facebook.com/h2hconference"
- In the last 3 years, the share of @gmail.com sender addresses in my inbox climbed to > 11% !!1!
  - Are you fucking kidding me?
- If the service is free, you are the product. Opfer!
  - At Google, 95% of all income, $43686 million
  - If you are too fucking lazy to read code, or set up a mail server, how about reading a report Form-10K?

SMTP for Dummies

```
whatever$ telnet kernelhacking.com 25
HELO phenoelit.de
MAIL FROM: <fx@phenoelit.de>
RCPT TO: <rodrigo@kernelhacking.com>
DATA
Subject: SMTP tutorial for the lambs

We are so going to party tonight!
.
QUIT
```

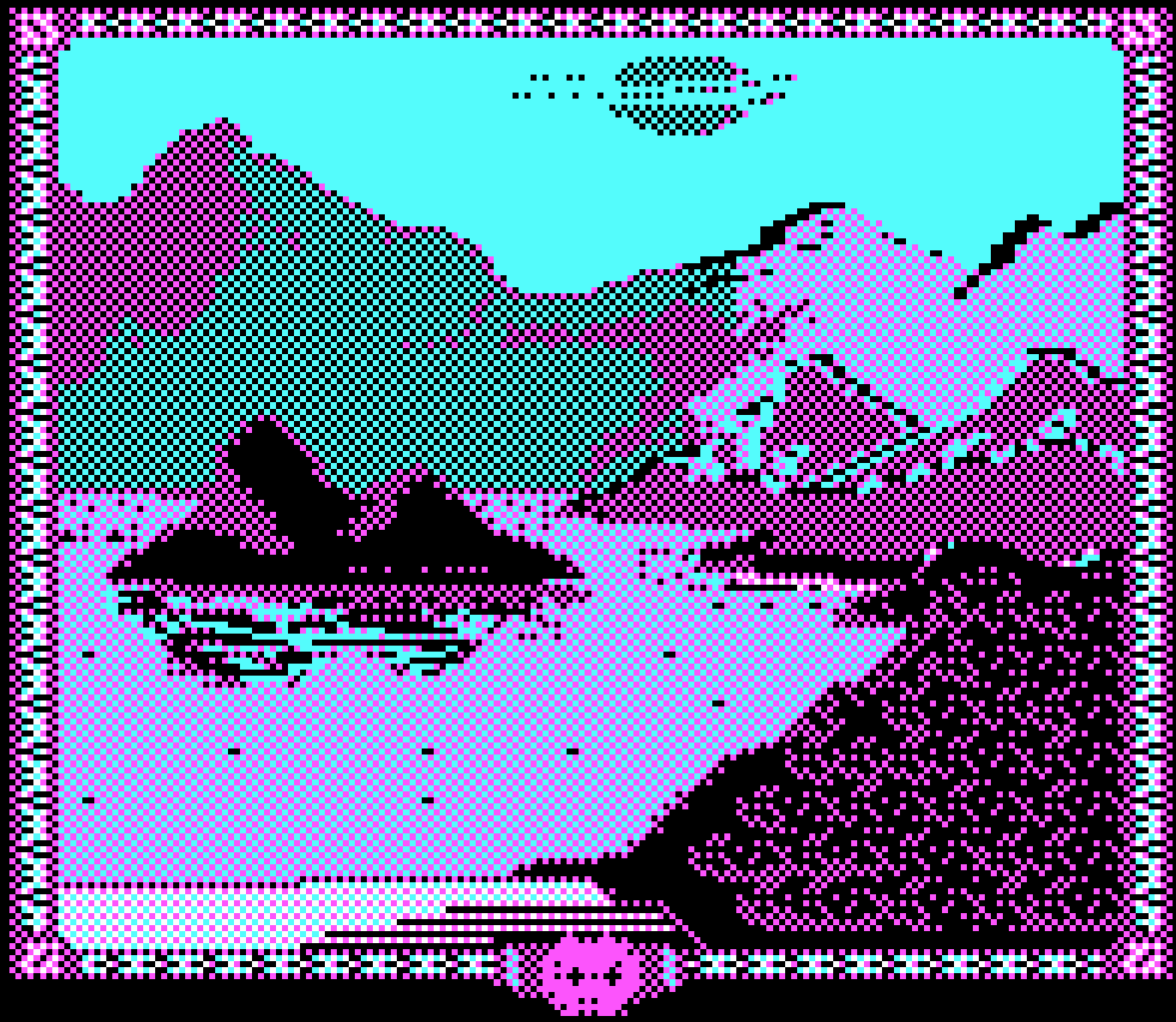
PGP Motherfuckers!



No one will do that!

- "OMG, the NSA reads my data on Google and Facebook!"
  - "My iPony is secure, everything in the AppStore is verified!"
- The concept ignored here is called SIGINT-Colonization
  - Amass control over enough devices, control points - ultimately people - and a more powerful force will seize your control
  - Getting your own country (e.g. North Korea) is not going to solve this
- This is maintaining options for states
  - You just make it easier for them by increasing your dependence willingly

It probably is, but WTF?



Meanwhile in the Shadows of Mordor

ID Please!

- All-encompassing mandatory identification online is on the way
  - In this case it's a shame to be German

Some people get everything X.509-signed.

CYBER WORLD PEACE
(MADE IN CHINA)

Submitted to the UN on September 12, 2011 by
China, Russia, Tajikistan and Uzbekistan

Code Of Conduct

- Not to use ICTs including networks to carry out hostile activities or acts of aggression and pose threats to international peace and security. Not to proliferate information weapons and related technologies.
- cooperate in combating criminal and terrorist activities which use ICTs [...]
  - [...] curbing dissemination of information which [...] undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment
- ensure the supply chain security of ICT products and services [...]
- respect the rights [...] and freedom of searching for, acquiring and disseminating information
- establishment of a multilateral, transparent and democratic international management of the Internet
- settle any dispute resulting from the application of this Code through peaceful means and refrain from the threat or use of force

Arms Control

- Washington D.C. recently changed its course on "cyber weapons"
  - International arms control for exploits and vulnerabilities, as if they were nukes
    - I'm sure Oracle and Apple have nothing to do with that whatsoever
- Think about it:
  - Where did Full Disclosure come from?
  - Why did it get traction?
  - Who saves money if it goes away?
    - Consider second order effects!
- Now consider the fallout
  - Are these WMDs on your computer, or are you just happy to cross our border?

Telephone Sanitizers

- Say "Cyber" and get budgets
  - Works in academia and governments
- Politicians and diplomats need technical advice, and badly so
  - Advice on defense comes from Symantec lobbyists
  - Advice on incident handling comes from HB Gary
  - Advice on network security comes from academia
  - Regulations come from the politicians
    - And the 4 companies that run the Internet
- I'm not aware of a single contribution from the offensive units of any State in international discussions

No ROM BASIC

The Root Cause: Product Liability

Don't bother with blinkered people.

Pride Ahead!

- Law Enforcement Organizations
  - "But we need this to catch criminals!"
  - "Privacy is less important than Security!"
  - "Nobody will have access to this data!"
  - "We only ask for what they have anyway."
- Pure Military
  - "This is secret, untouchable"
  - "Politically, we cannot do that"
  - "The private sector is less important"
  - "You are fat, fuck off"
- If it feels like an arrogant idiot, it probably is one.

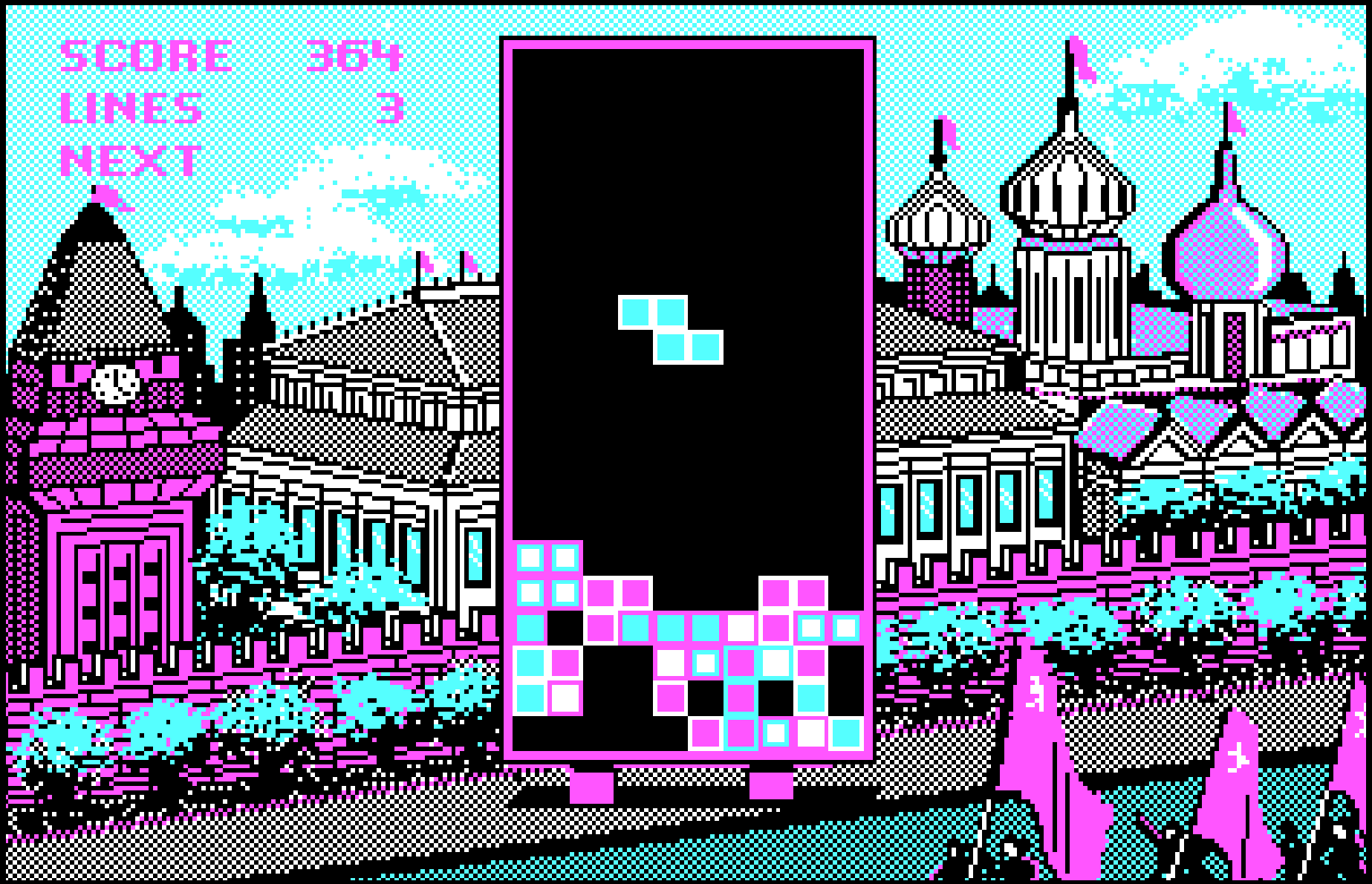
Expect Ingratitude

What Now?

Imagine, you could actually change things?

Politics Built In

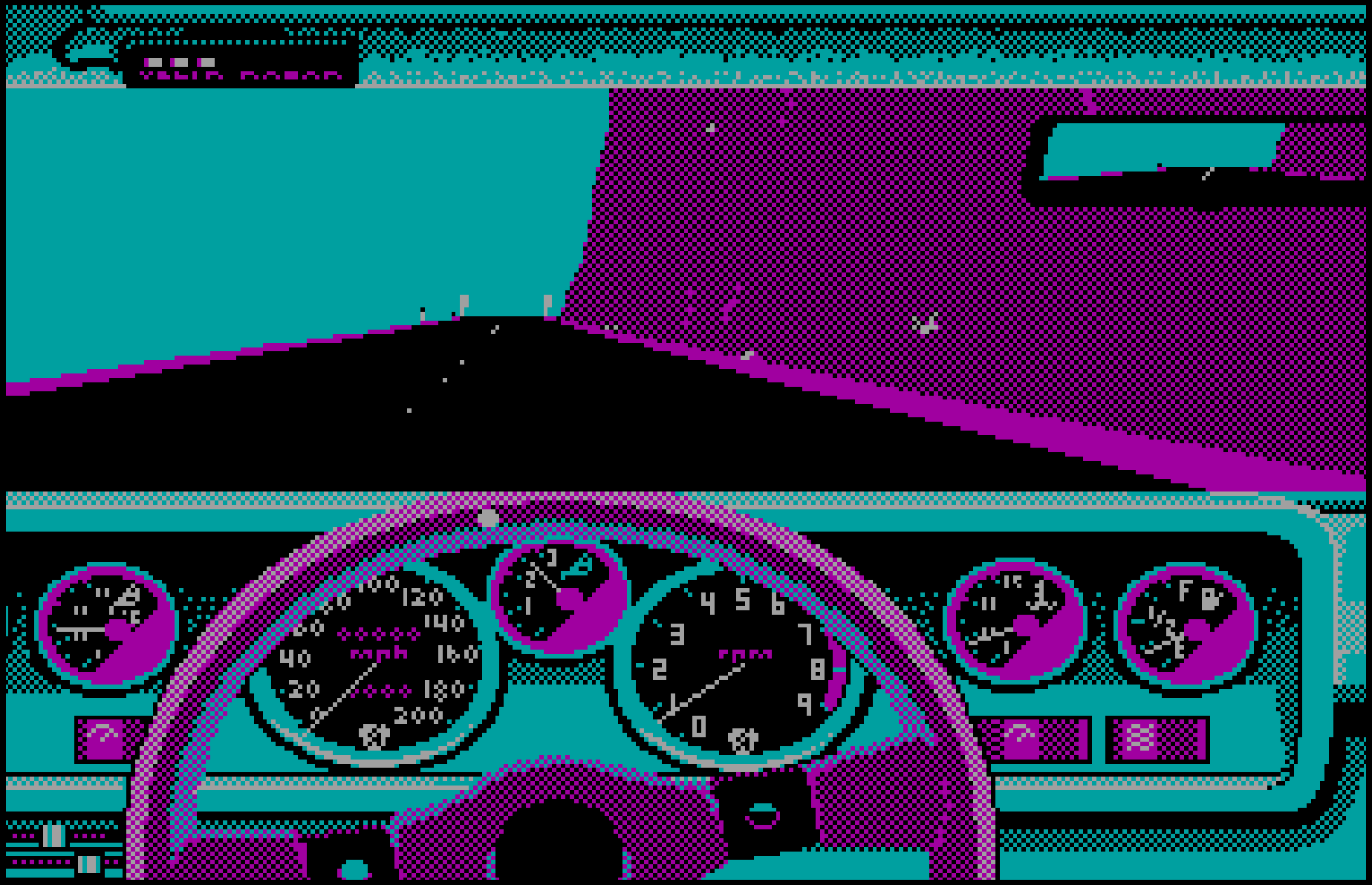
- Evi Nemeth (*1940 – †2013) had it right
- It's all about going the whole nine layers!
- You grew up
  - Job + Money
  - Family
  - Kids
- How about some sense of responsibility to go with that?



Success evaporates fast
Failures pile up

Research for Peace

- Every vulnerability published is a weapon taken away from someone
- Turing tests, not CAPTCHAs, allow to show that you didn't do something
- Design every interface you build by LangSec rules, or die in a fire
- Authorization rarely needs full ID – people you don't trust do
- Also, we need components that are recoverable from compromise
  - Please! ☺



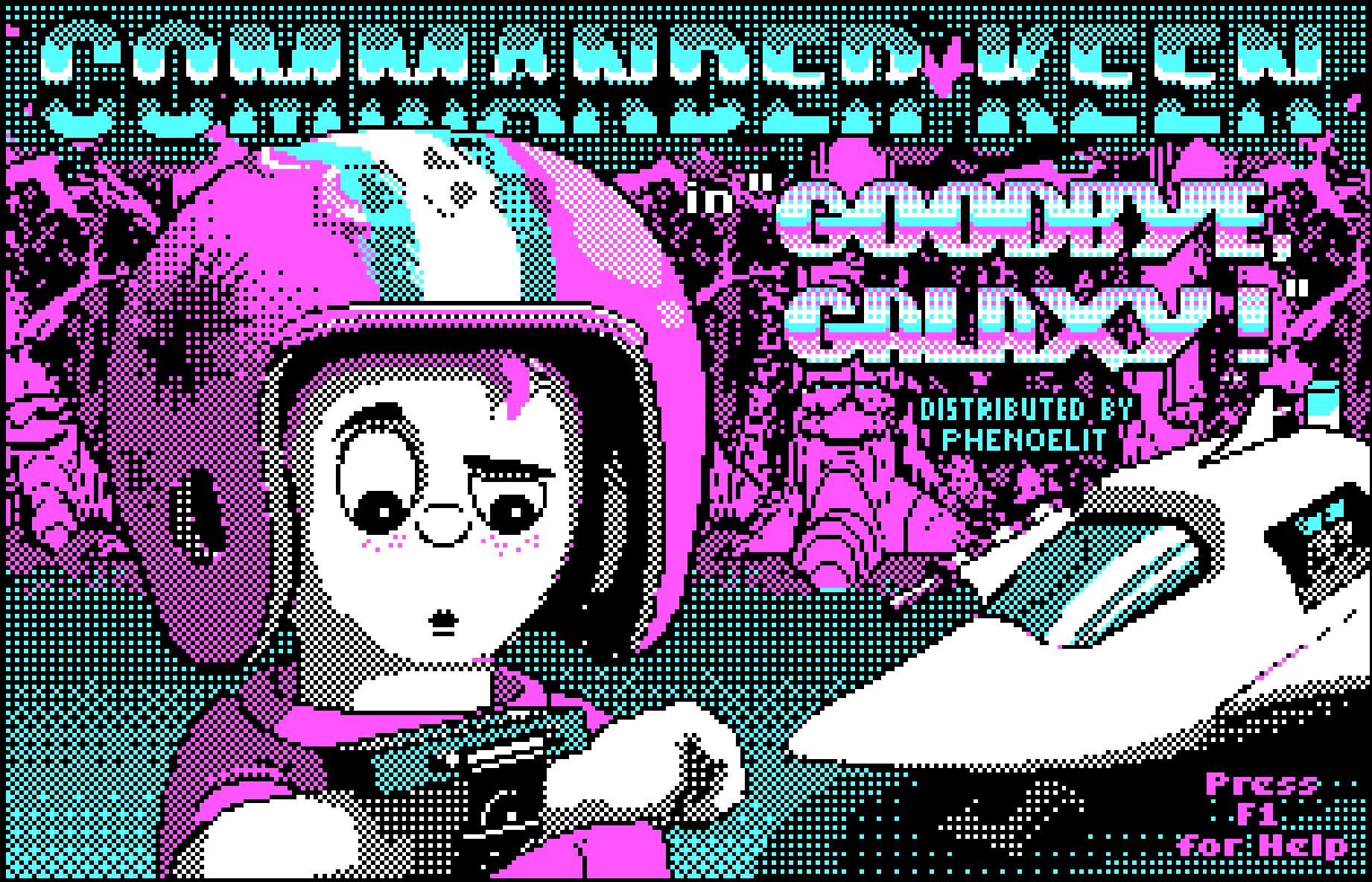
Driving around in a Prius on TV isn't helping.
#include <other_things_it_is_not.h>

The Elders Shake Their Head at Us

+ Politics are almost as exciting as war, and quite as dangerous ... In war, you can only be killed once. But in politics many times.
  + Sounds familiar?
+ Indeed, it has been said that democracy is the worst form of government except all those other forms that have been tried from time to time.
+ When haters are "speechless", it takes them three blog posts to express it.
  + Yes, I paraphrased that one. Sorry ;)

Sir Winston Leonard Spencer-Churchill

Yes, it's up to us now.



Am I over time?