Software Security Principles, con’t

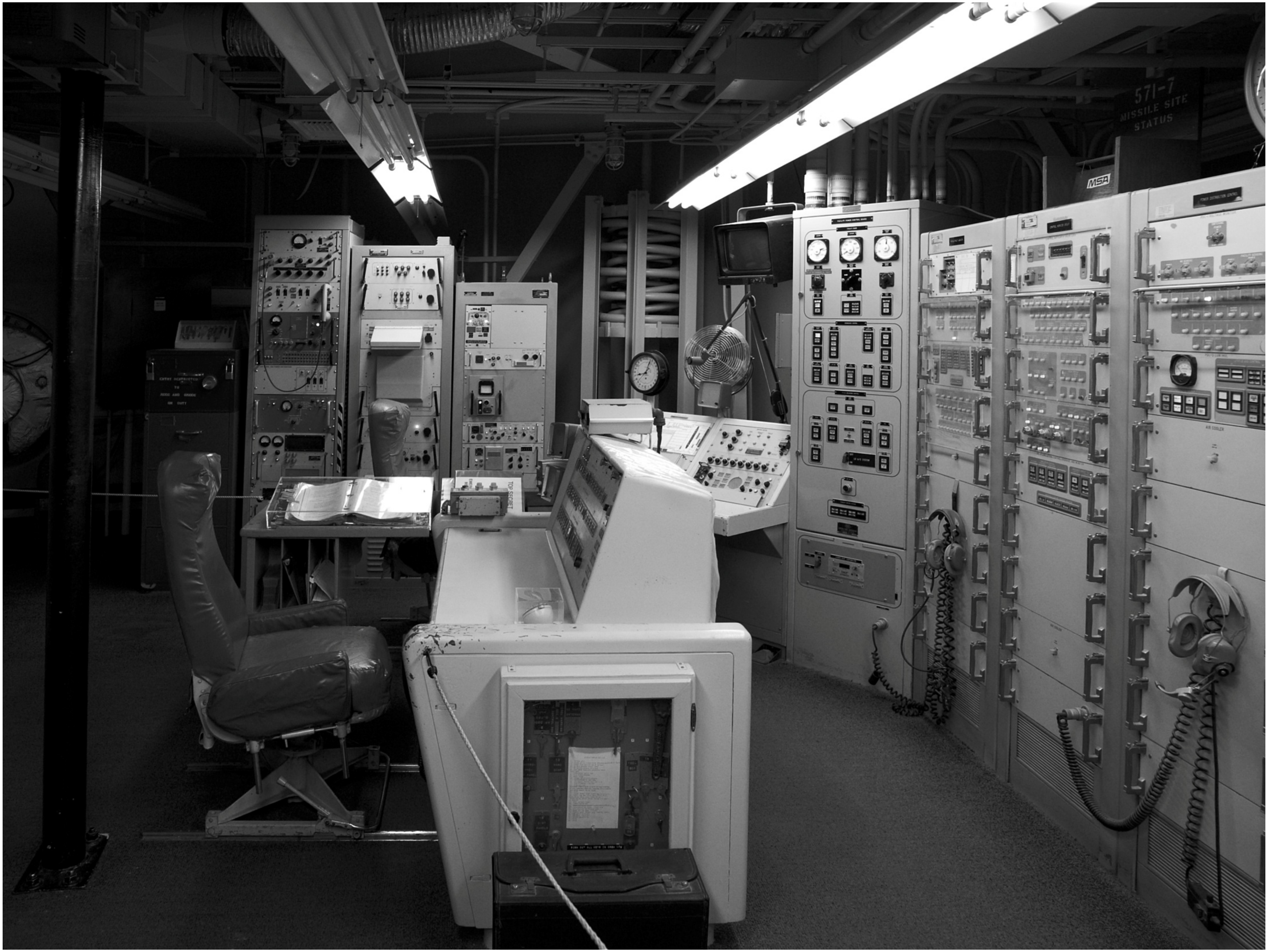
CS 161: Computer Security

Prof. Vern Paxson

TAs: Devdatta Akhawe, Mobin Javed & Matthias Vallentin

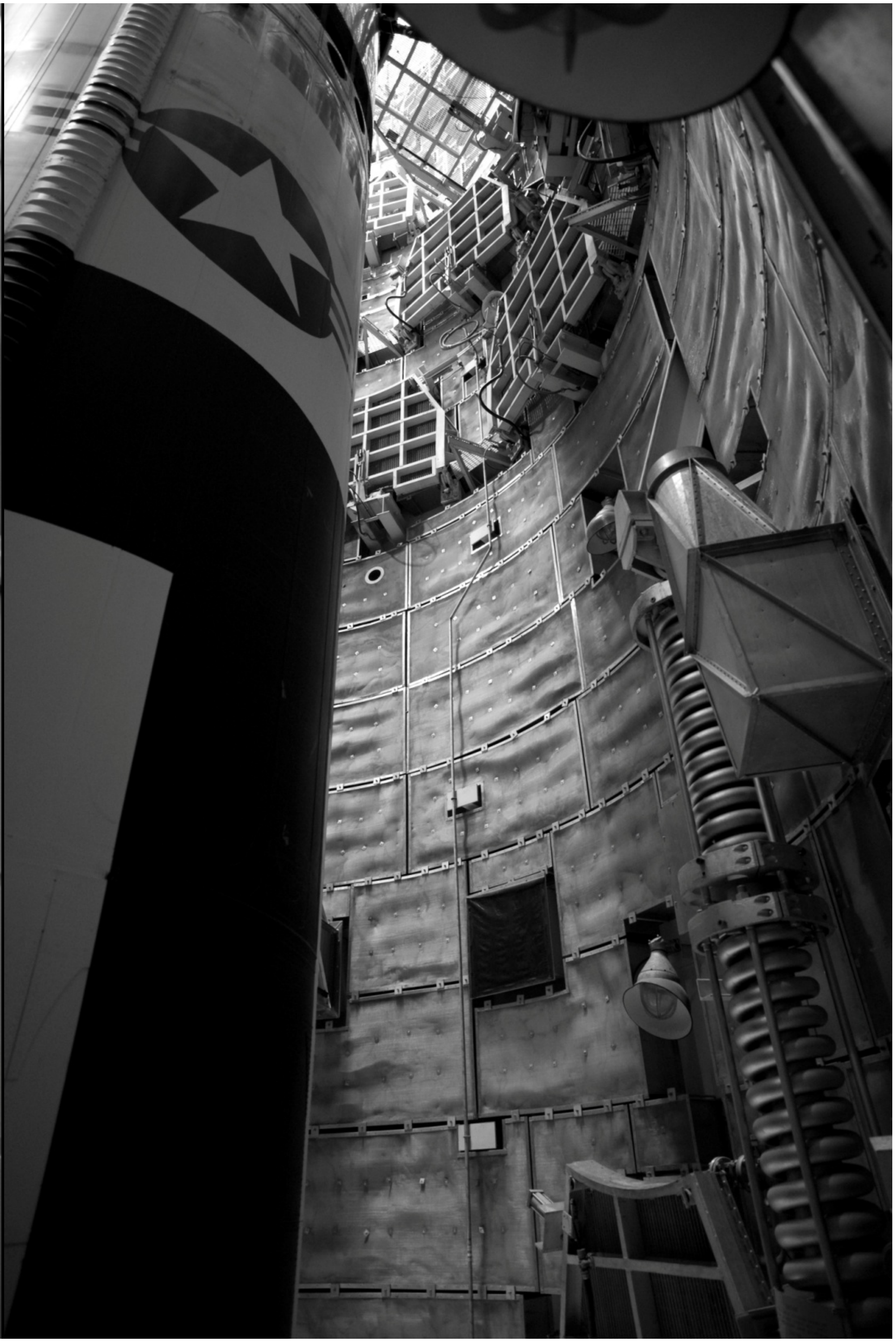
http://inst.eecs.berkeley.edu/~cs161/

January 27, 2011



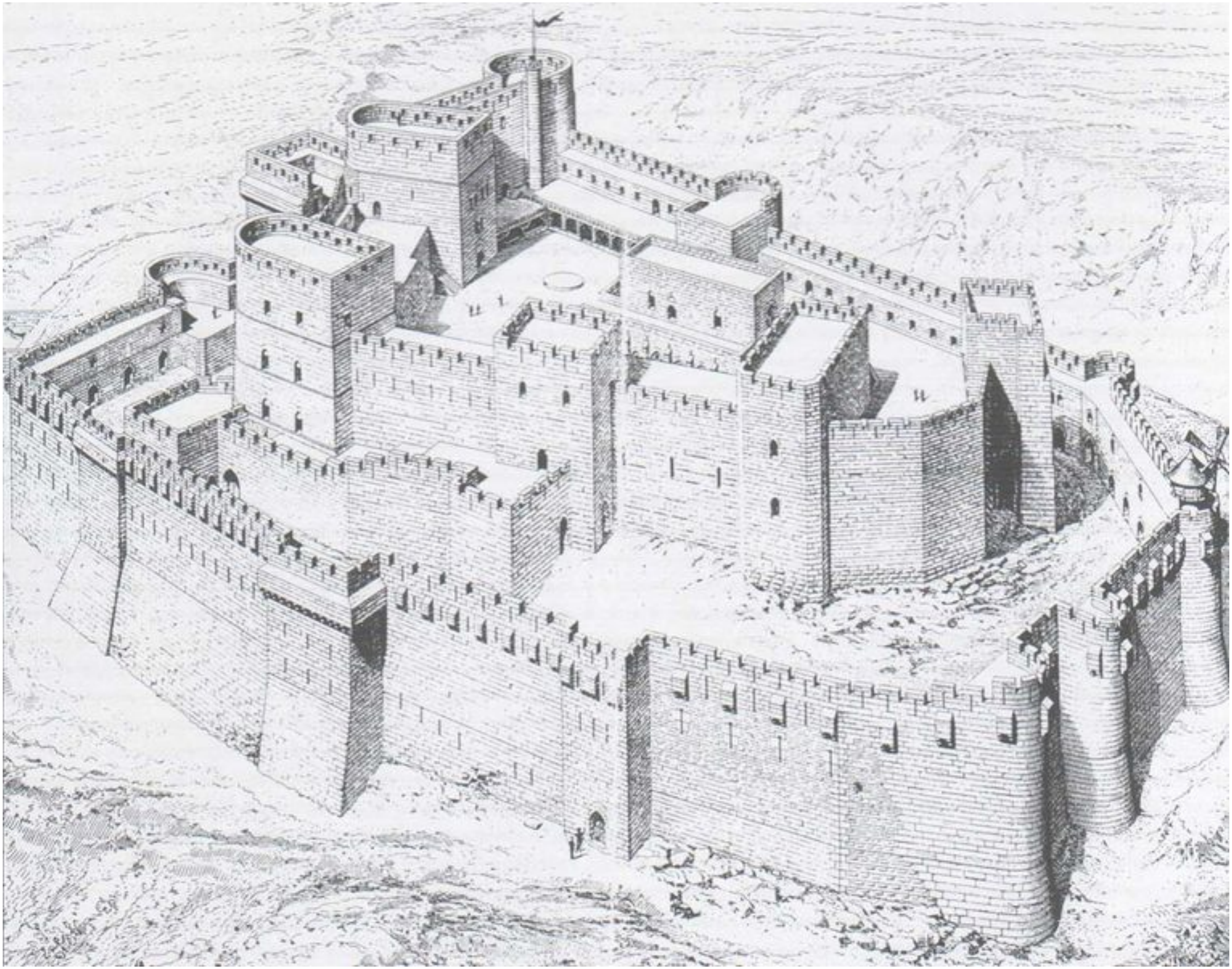
571-7
MISSILE SITE
STATUS
MSA
TOP SECRET

NO LONE ZONE
SAC TWO MAN POLICY
MANDATORY
CAUTION
DO NOT KEY RTMX IN L/D
EXCEPT IN CASE OF AN
EMERGENCY-MUST BE AT
LEAST 5FT FROM MSL.
E-F-G



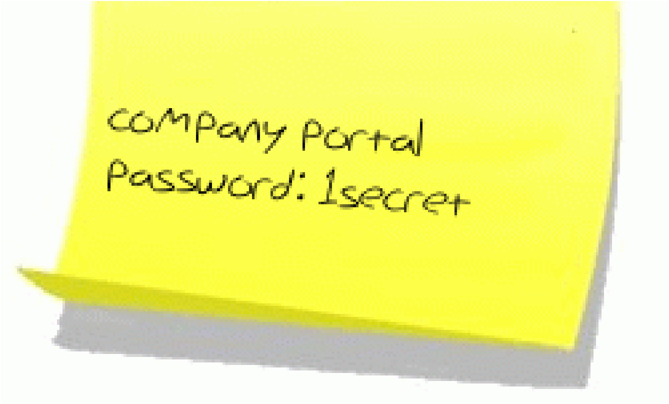
TICKET
356011

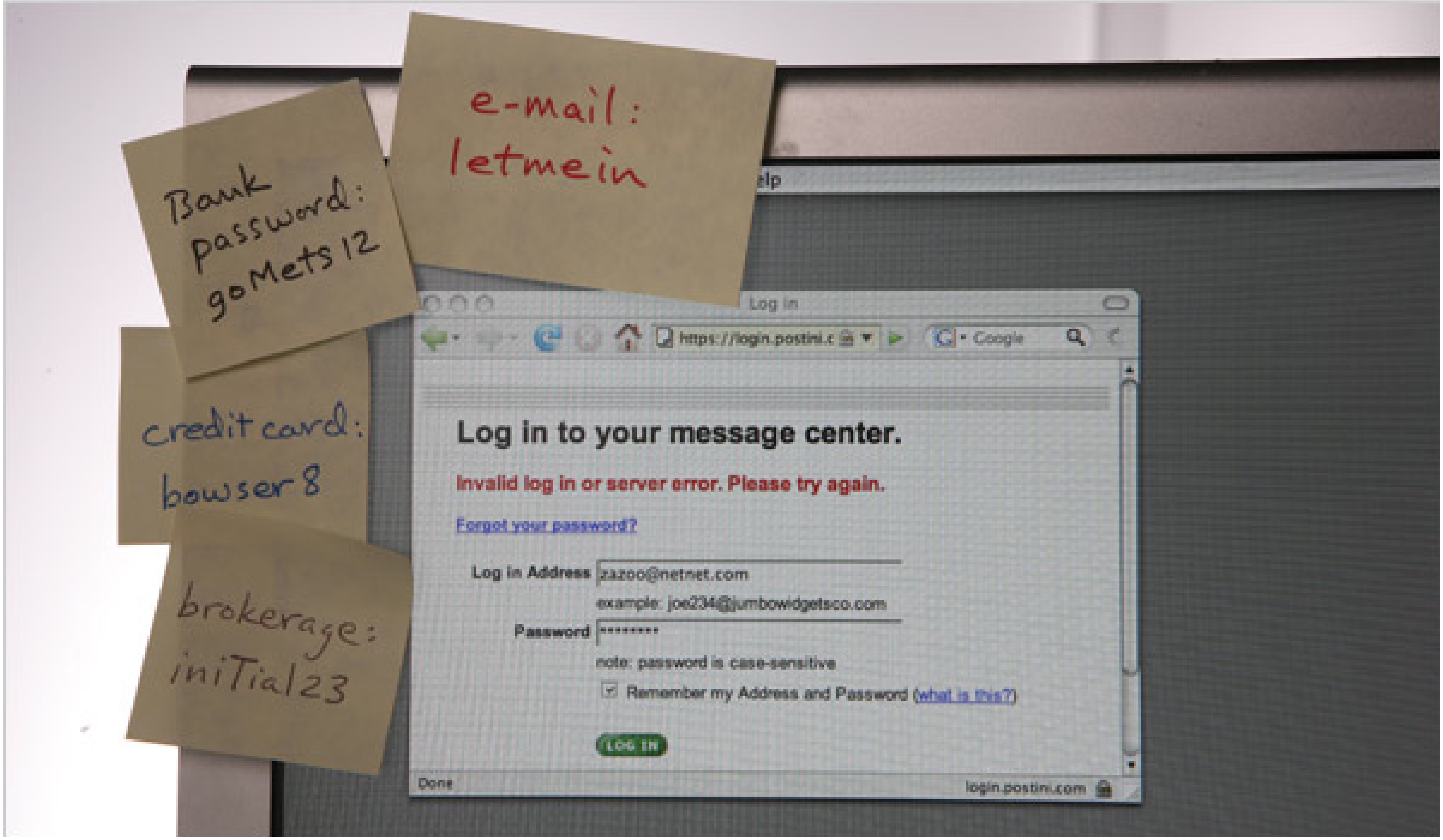
“Separation of responsibility.”



“Defense in depth.”

“Company policy: passwords must be at least 10 characters long, contain at least 2 digits, 1 uppercase character, 1 lowercase character, and 1 special character.”





Log in to your message center.

Invalid log in or server error. Please try again.

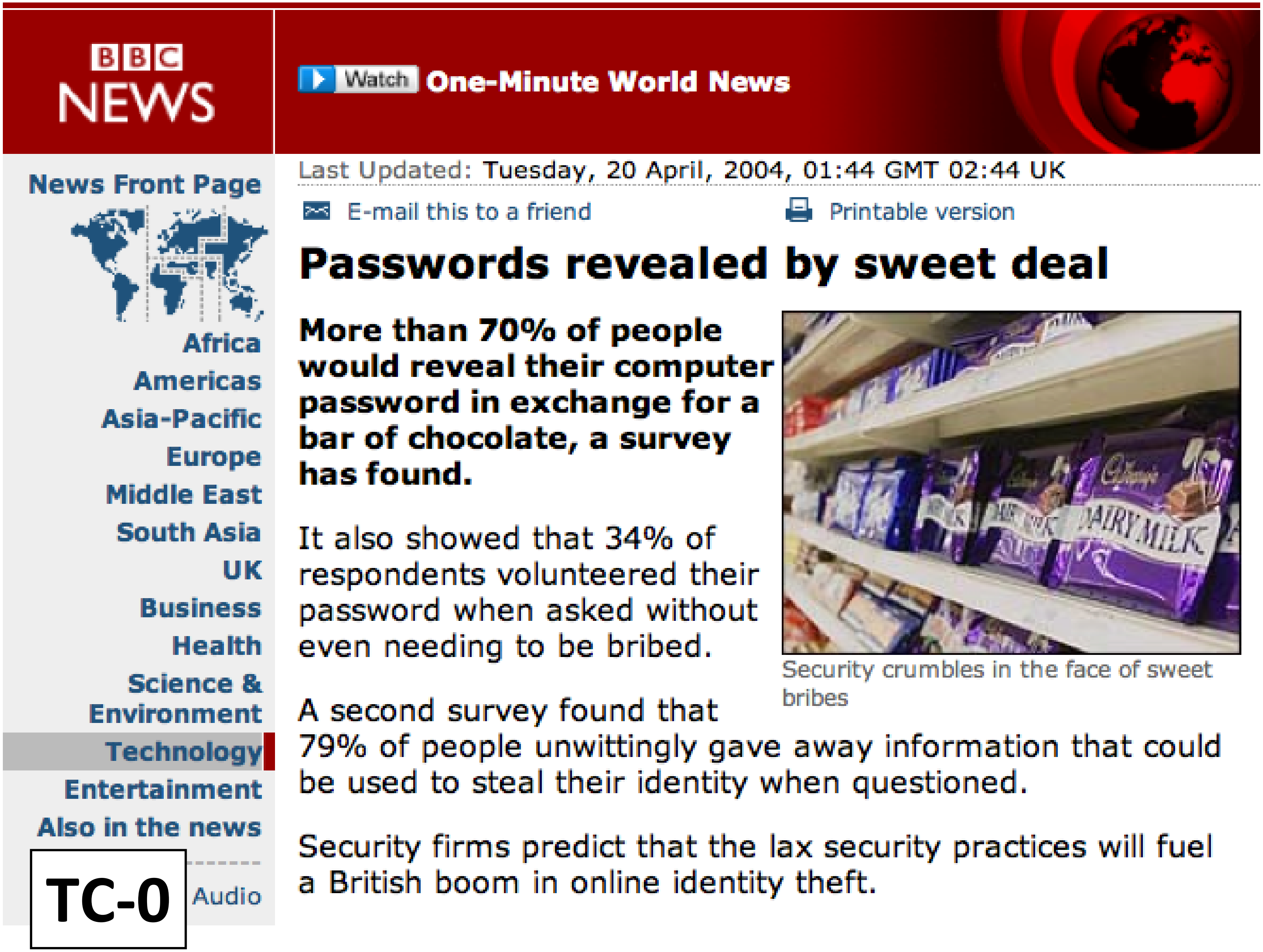
Log in Address zazoo@netnet.com

example: joe234@jumbowidgetsco.com

Password *********

note: password is case-sensitive

☑ Remember my Address and Password (what is this?)



Last Updated: Tuesday, 20 April, 2004, 01:44 GMT 02:44 UK

Passwords revealed by sweet deal

More than 70% of people would reveal their computer password in exchange for a bar of chocolate, a survey has found.

It also showed that 34% of respondents volunteered their password when asked without even needing to be bribed.

A second survey found that 79% of people unwittingly gave away information that could be used to steal their identity when questioned.

Security firms predict that the lax security practices will fuel a British boom in online identity theft.

Security crumbles in the face of sweet bribes

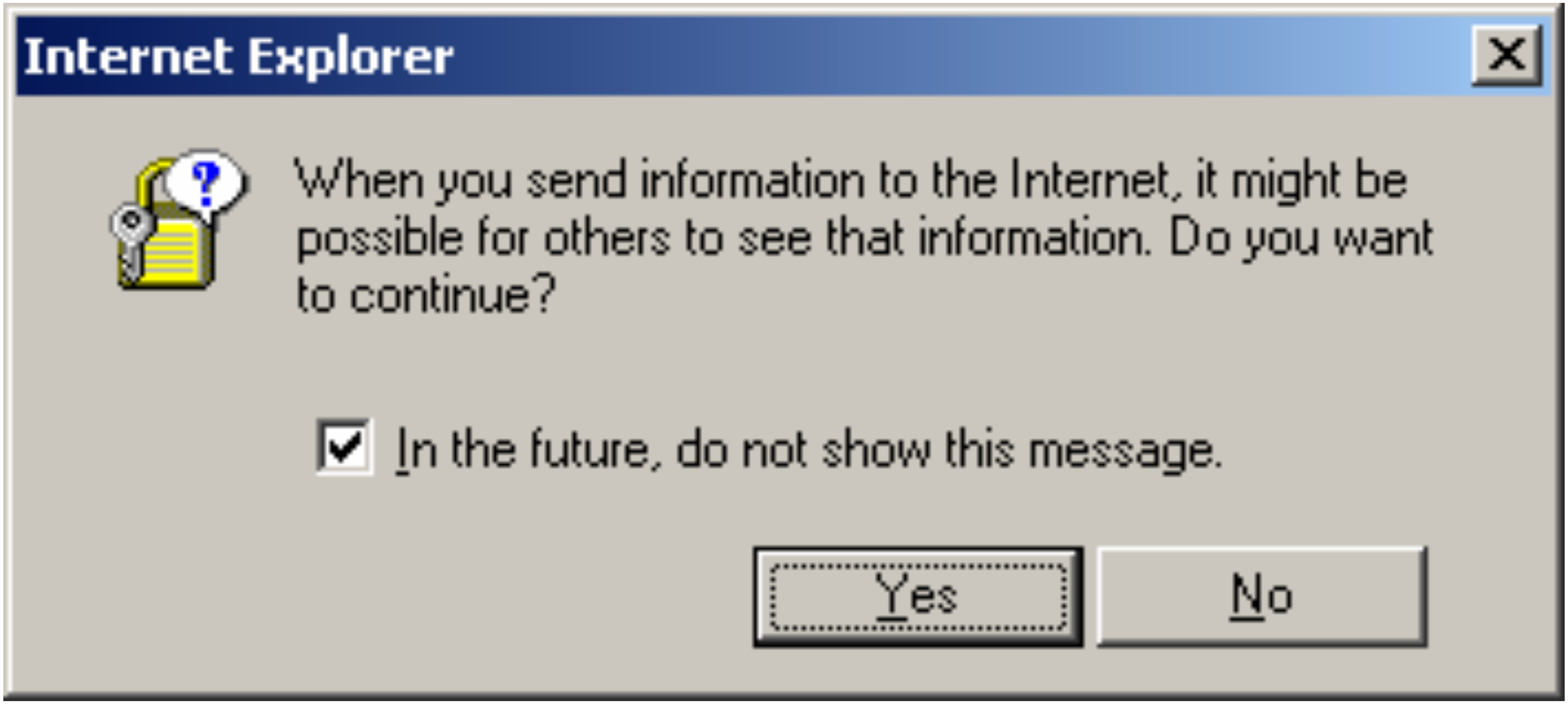
TC-0

What a piece of work is a man! how Noble in
Reason! how infinite in faculty! in form and moving
how express and admirable! in Action, how like an Angel!
in apprehension, how like a God!
-- *Hamlet* Act II, Scene II

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)"

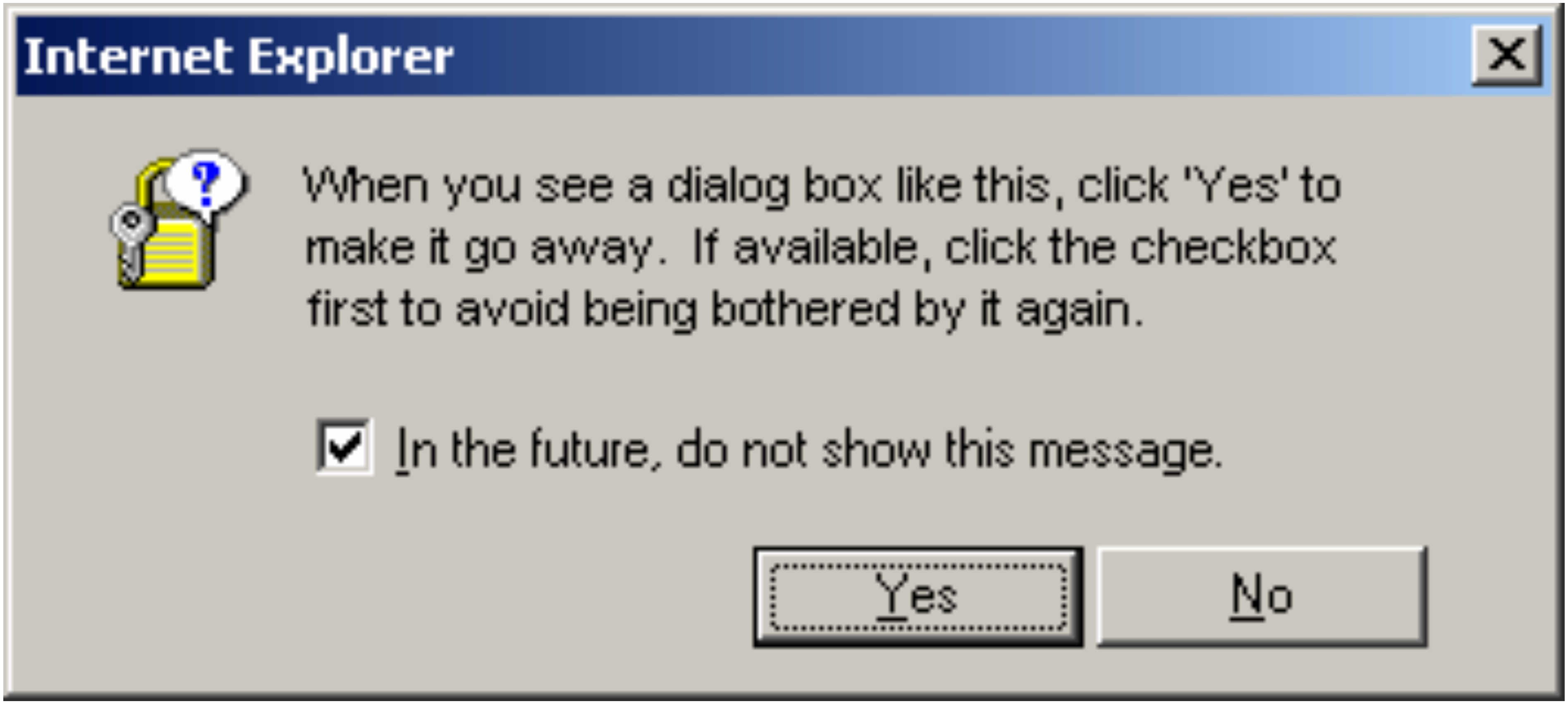
-- *Network Security: Private Communication in a Public World*,
Charlie Kaufman, Radia Perlman, & Mike Speciner, 1995

“Psychological acceptability.”



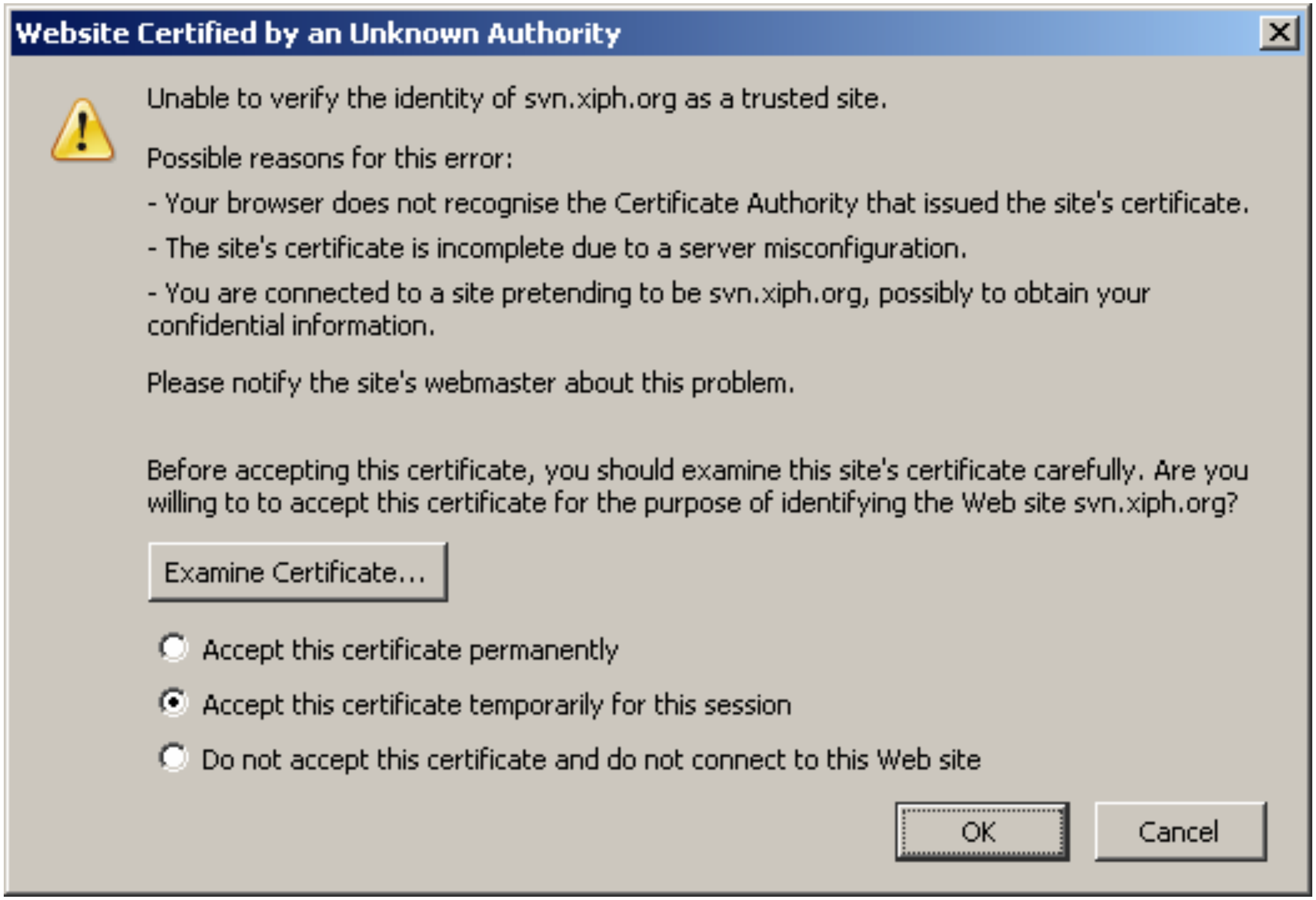
When you send information to the Internet, it might be possible for others to see that information. Do you want to continue?

☑ In the future, do not show this message.



When you see a dialog box like this, click 'Yes' to make it go away. If available, click the checkbox first to avoid being bothered by it again.

☑ In the future, do not show this message.



Website Certified by an Unknown Authority

Unable to verify the identity of svn.xiph.org as a trusted site.

Possible reasons for this error:

- Your browser does not recognise the Certificate Authority that issued the site's certificate.

- The site's certificate is incomplete due to a server misconfiguration.

- You are connected to a site pretending to be svn.xiph.org, possibly to obtain your confidential information.

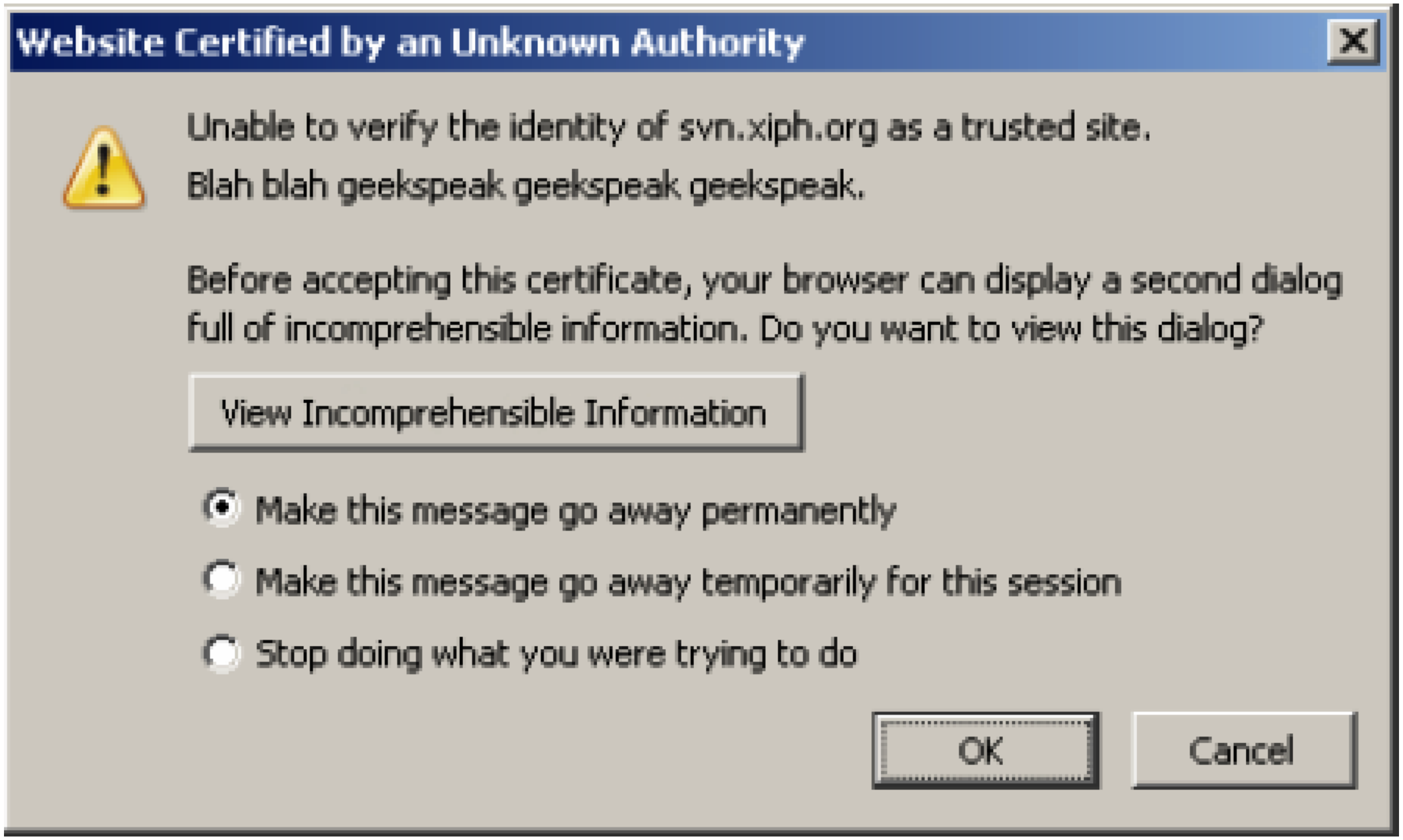
Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site svn.xiph.org?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this Web site



Website Certified by an Unknown Authority

Unable to verify the identity of svn.xiph.org as a trusted site.

Blah blah geekspeak geekspeak geekspeak.

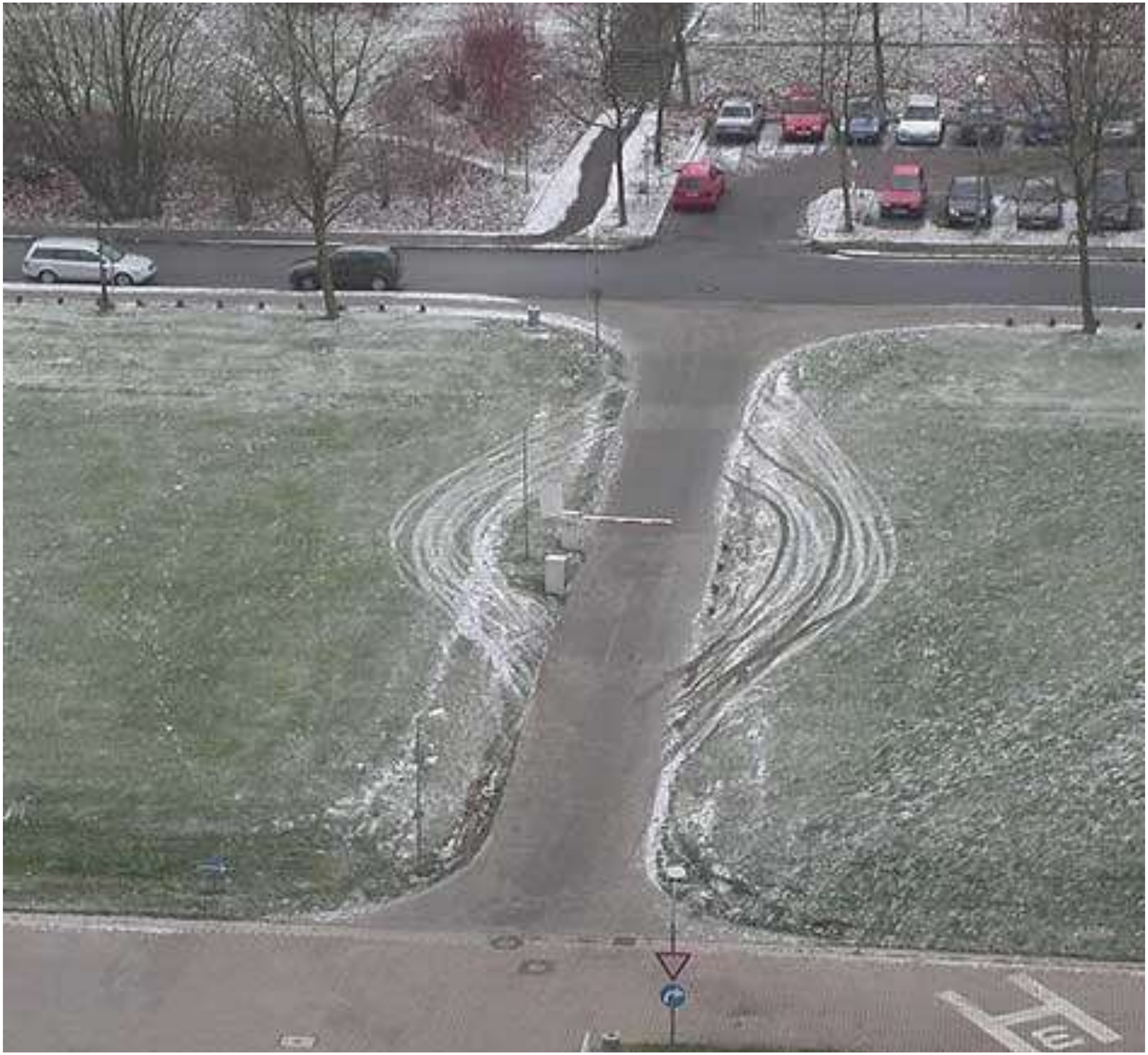
Before accepting this certificate, your browser can display a second dialog full of incomprehensible information. Do you want to view this dialog?

● Make this message go away permanently

○ Make this message go away temporarily for this session

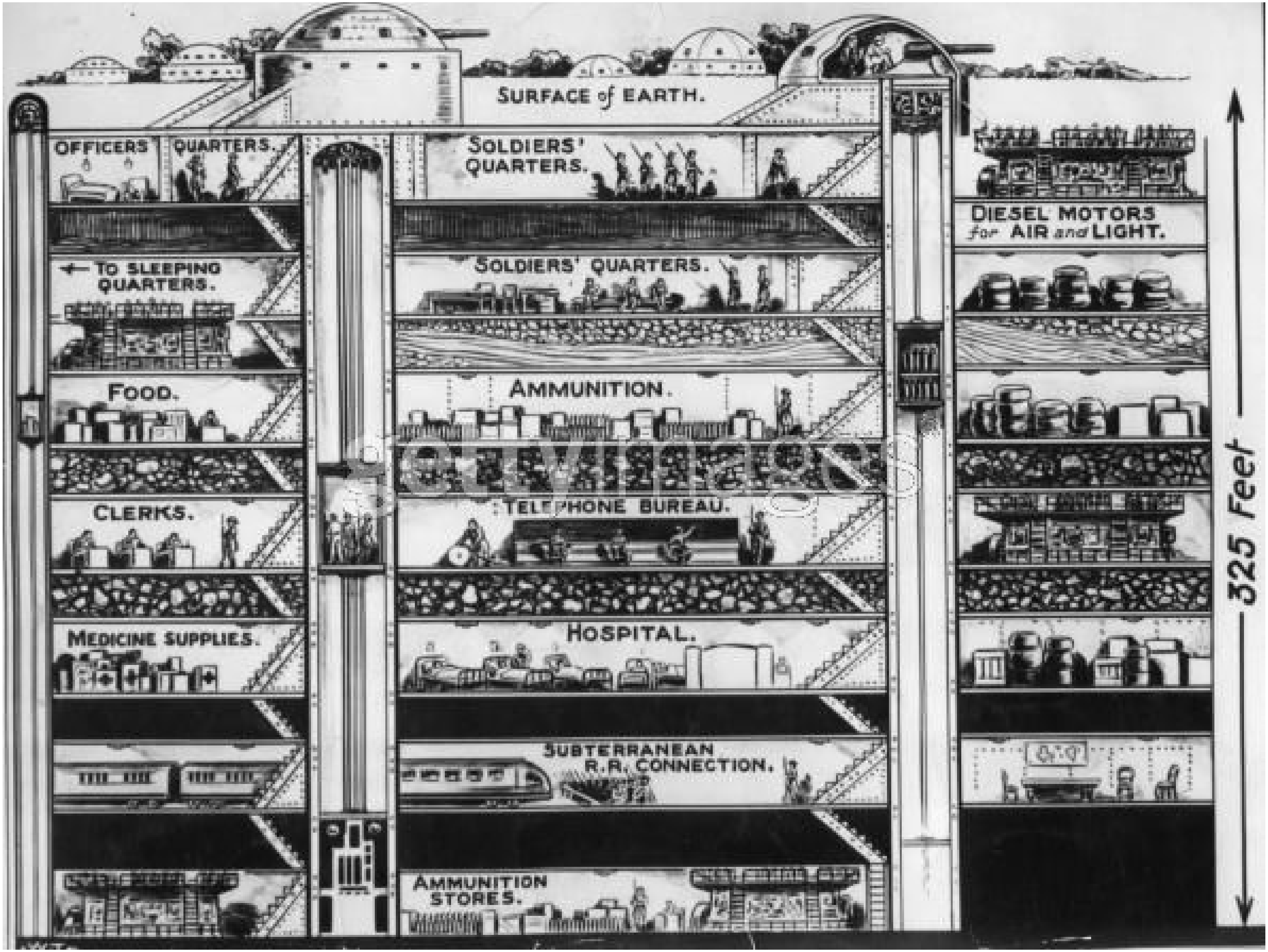
○ Stop doing what you were trying to do

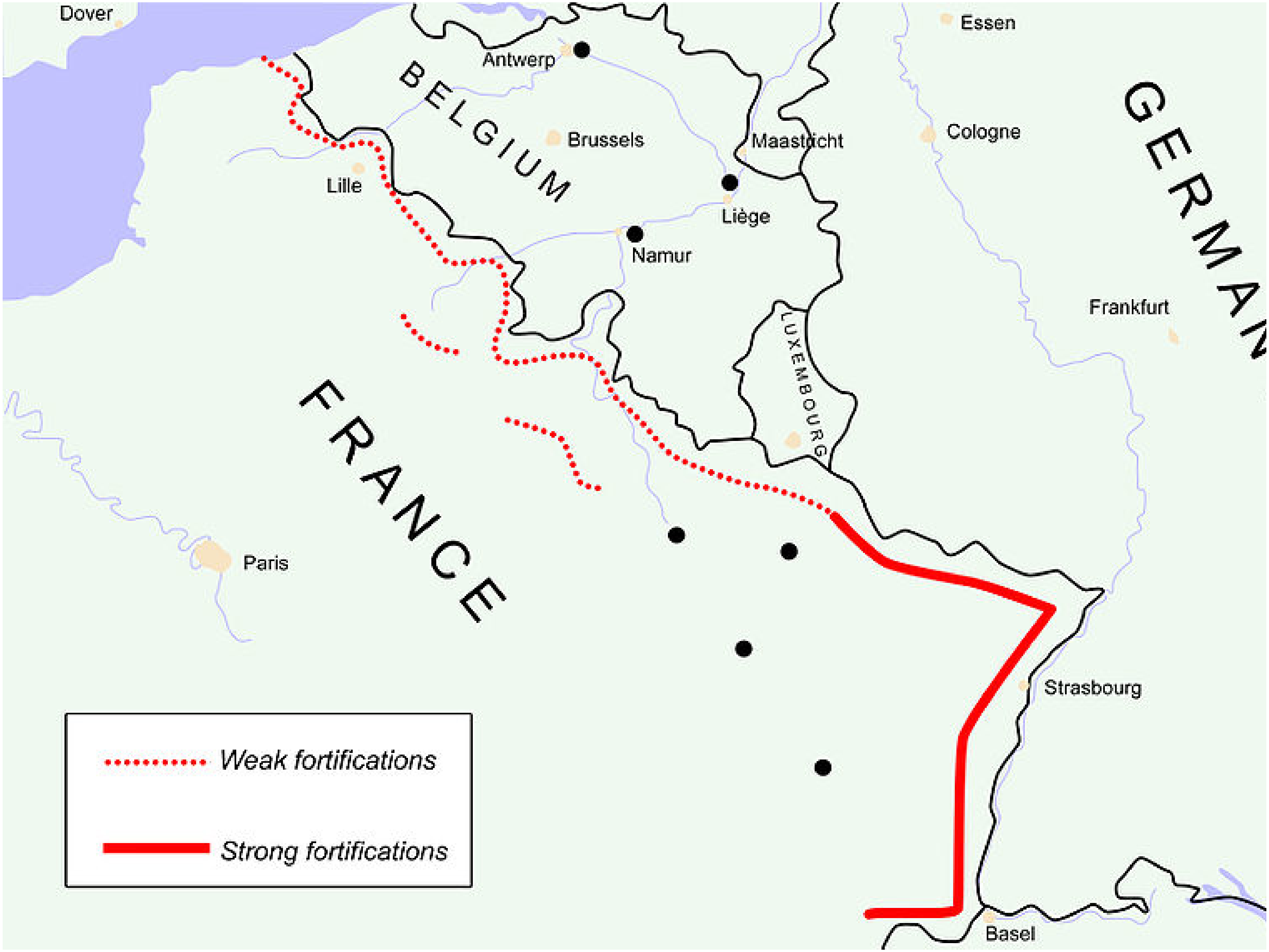
“Consider human factors.”

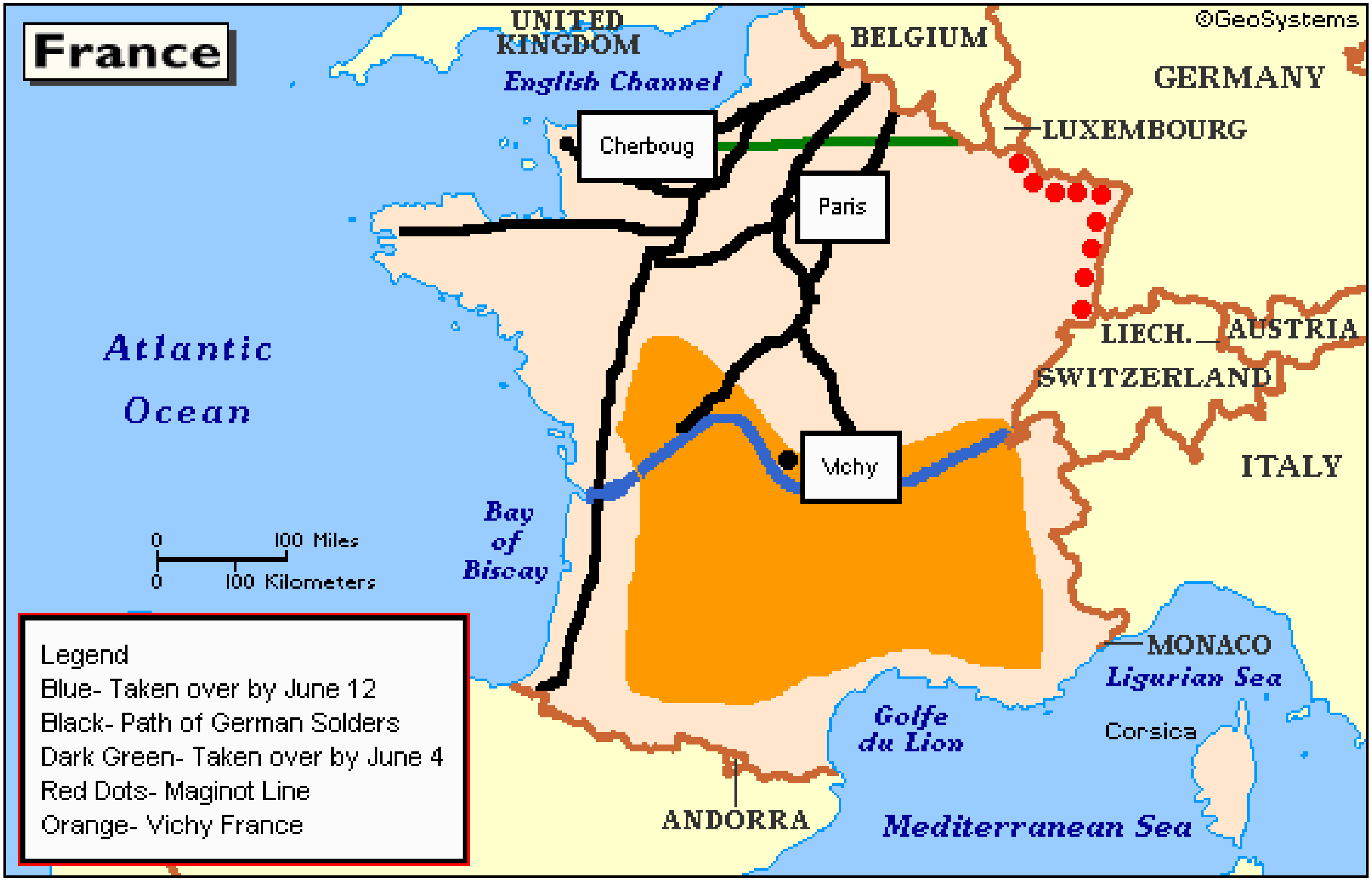


“Ensure complete mediation.”

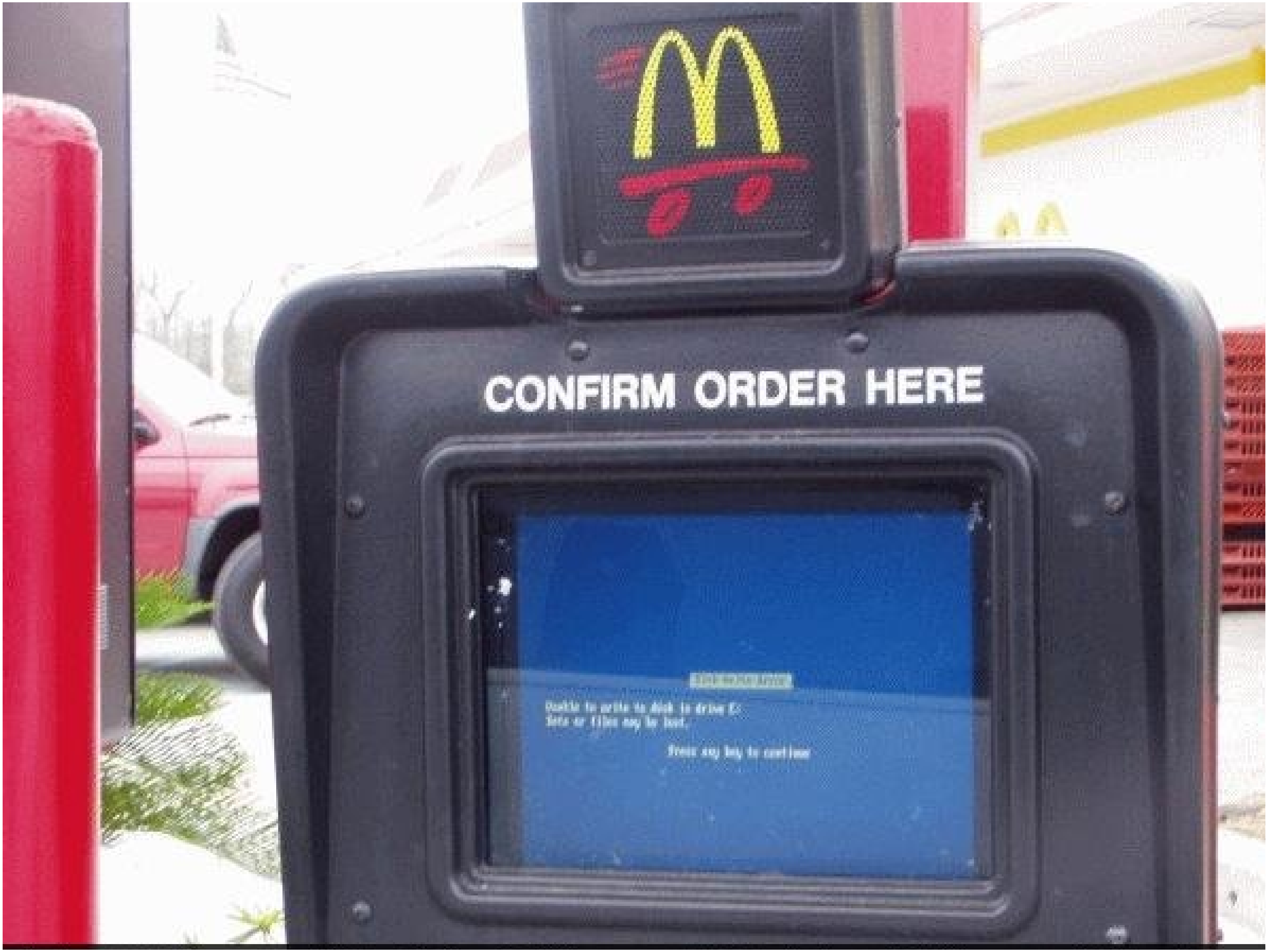
2


SURFACE of EARTH.
OFFICERS' QUARTERS.
SOLDIERS' QUARTERS.
DIESEL MOTORS for AIR and LIGHT.
← TO SLEEPING QUARTERS.
SOLDIERS' QUARTERS.
FOOD.
AMMUNITION.
CLERKS.
TELEPHONE BUREAU.
MEDICINE SUPPLIES.
HOSPITAL.
SUBTERRANEAN R.R. CONNECTION.
AMMUNITION STORES.
325 Feet

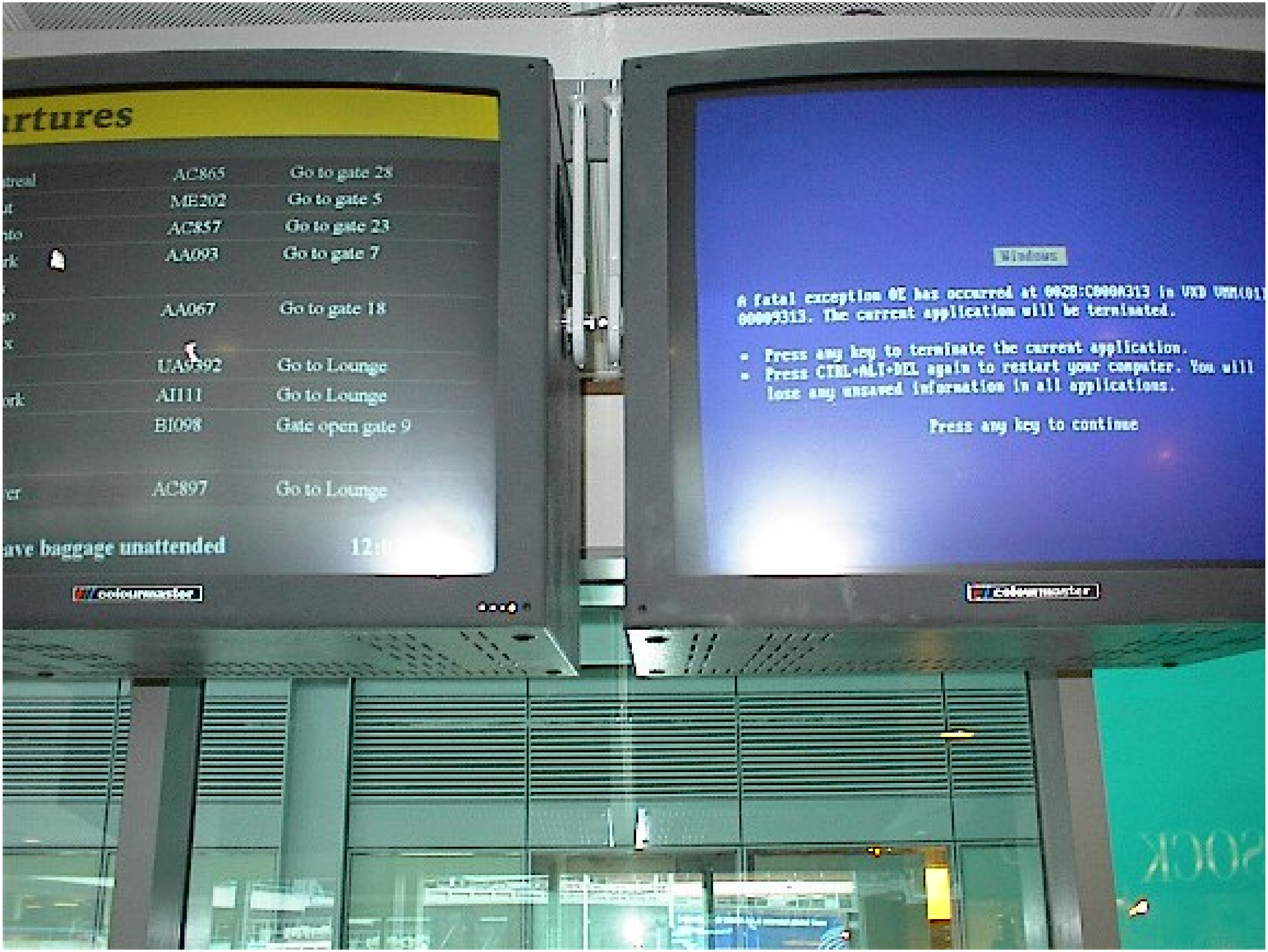

Dover
Antwerp
Essen
BELGIUM
Brussels
Maastricht
Cologne
GERMAN
Lille
Liège
Namur
Frankfurt
LUXEMBOURG
FRANCE
Paris
Strasbourg
Basel
Weak fortifications
Strong fortifications


France
©GeoSystems
UNITED KINGDOM
English Channel
BELGIUM
GERMANY
LUXEMBOURG
Cherboug
Paris
Vichy
LIECH.
AUSTRIA
SWITZERLAND
ITALY
Atlantic Ocean
Bay of Biscay
0 100 Miles
0 100 Kilometers
MONACO
Ligurian Sea
Corsica
Golfe du Lion
ANDORRA
Mediterranean Sea
Legend
Blue- Taken over by June 12
Black- Path of German Solders
Dark Green- Taken over by June 4
Red Dots- Maginot Line
Orange- Vichy France

“Don’t fight the last war.”



```
[illegible]
Unable to write to disk in drive C:
Data or files may be lost.

            Press any key to continue
```

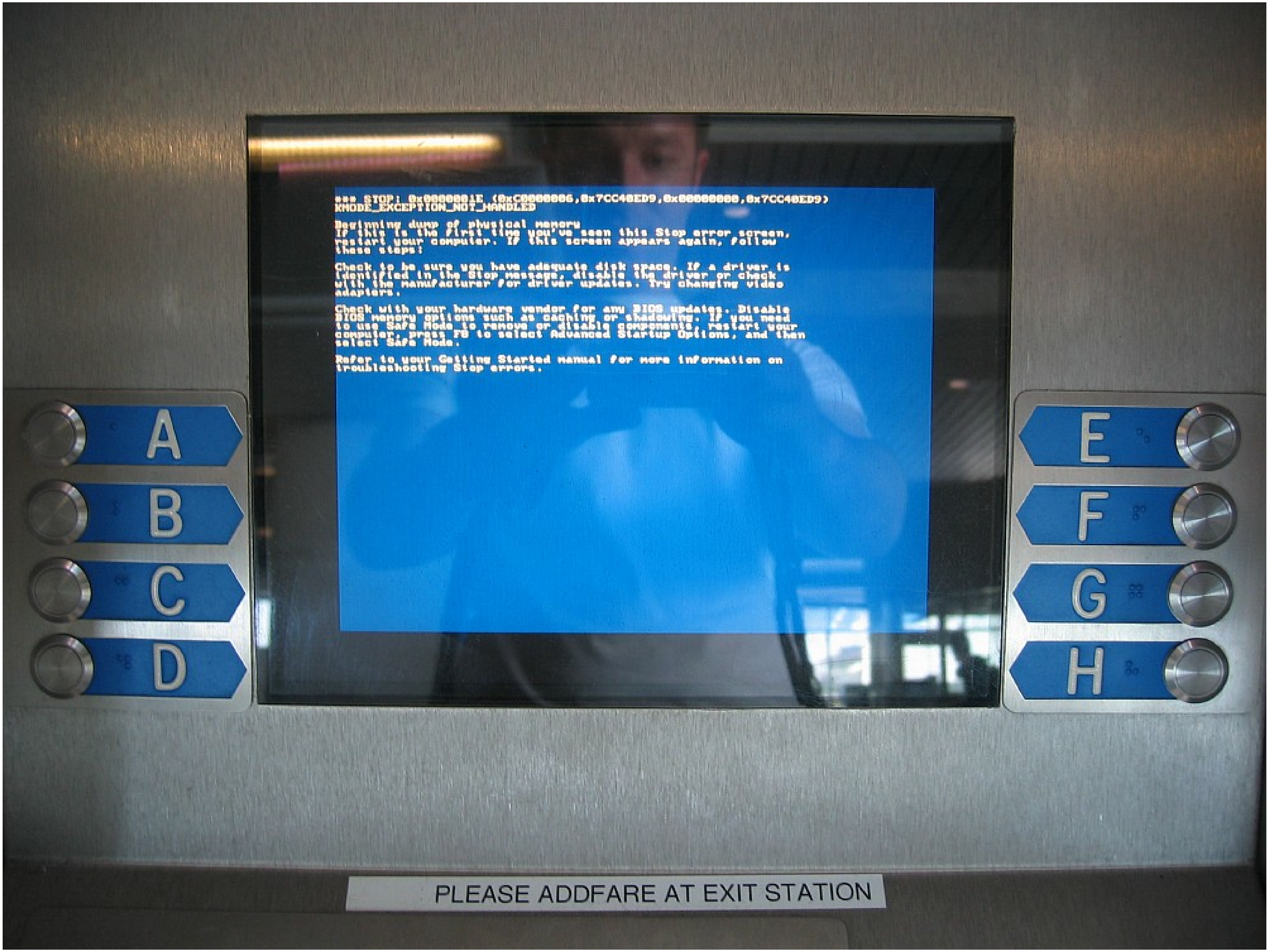


rtures

treal	AC865	Go to gate 28
t	ME202	Go to gate 5
nto	AC857	Go to gate 23
rk	AA093	Go to gate 7
s		
go	AA067	Go to gate 18
x		
	UA9392	Go to Lounge
ork	AI111	Go to Lounge
	BI098	Gate open gate 9
er	AC897	Go to Lounge

ave baggage unattended 12:0

```
                          Windows

A fatal exception 0E has occurred at 0028:C000A313 in VXD VMM(01)
00009313. The current application will be terminated.

*  Press any key to terminate the current application.
*  Press CTRL+ALT+DEL again to restart your computer. You will
   lose any unsaved information in all applications.

                  Press any key to continue
```



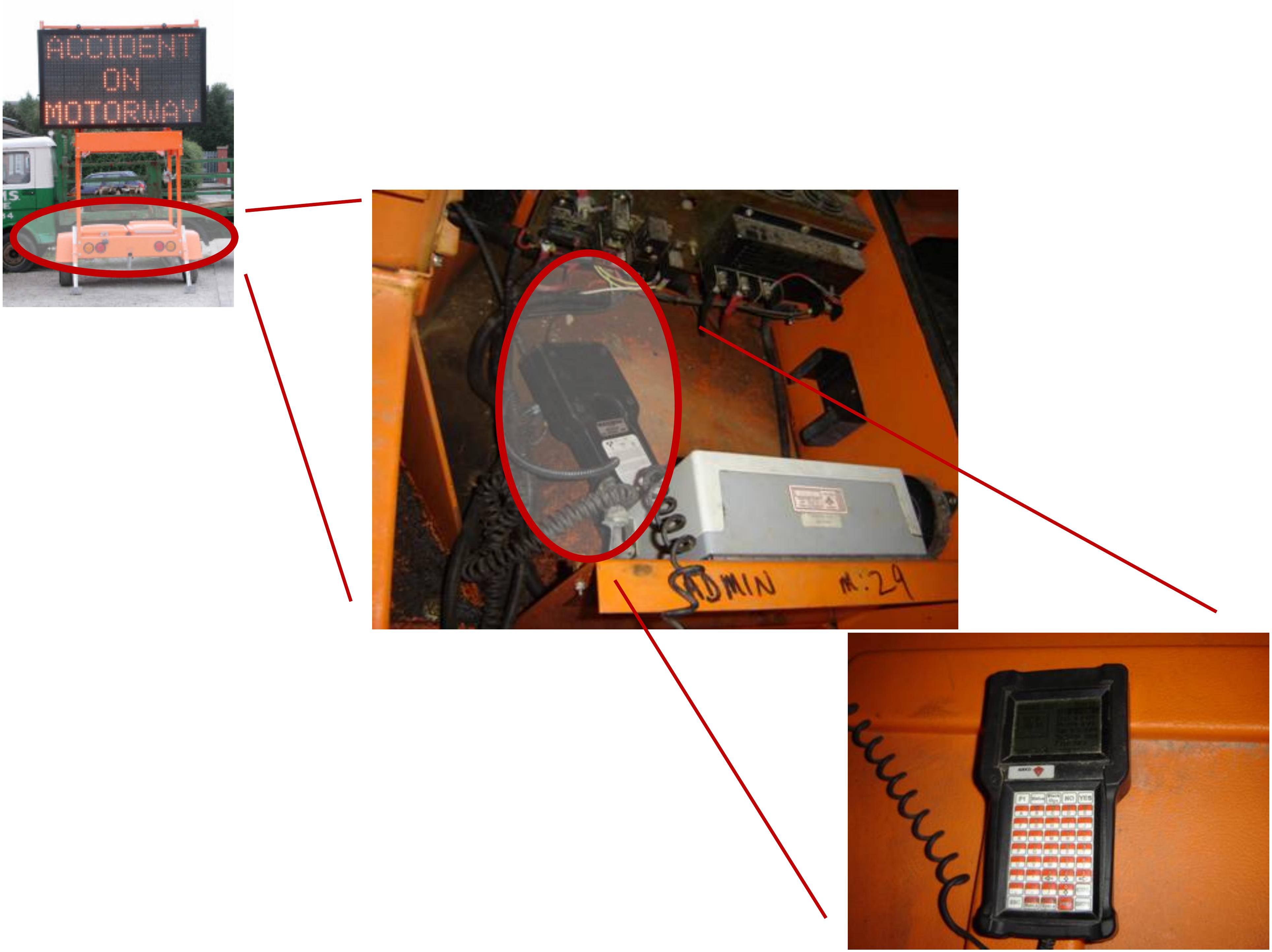
```
*** STOP: 0x0000001E (0xC0000006,0x7CC40ED9,0x00000000,0x7CC40ED9)
KMODE_EXCEPTION_NOT_HANDLED

Beginning dump of physical memory
If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to be sure you have adequate disk space. If a driver is
identified in the Stop message, disable the driver or check
with the manufacturer for driver updates. Try changing video
adapters.

Check with your hardware vendor for any BIOS updates. Disable
BIOS memory options such as caching or shadowing. If you need
to use Safe Mode to remove or disable components, restart your
computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Refer to your Getting Started manual for more information on
troubleshooting Stop errors.
```

ATM
My Computer
Windows Media Player
Network Neighborhood
Inbox
Internet Explorer
Recycle Bin
My Briefcase
Start

“Threat models change.”

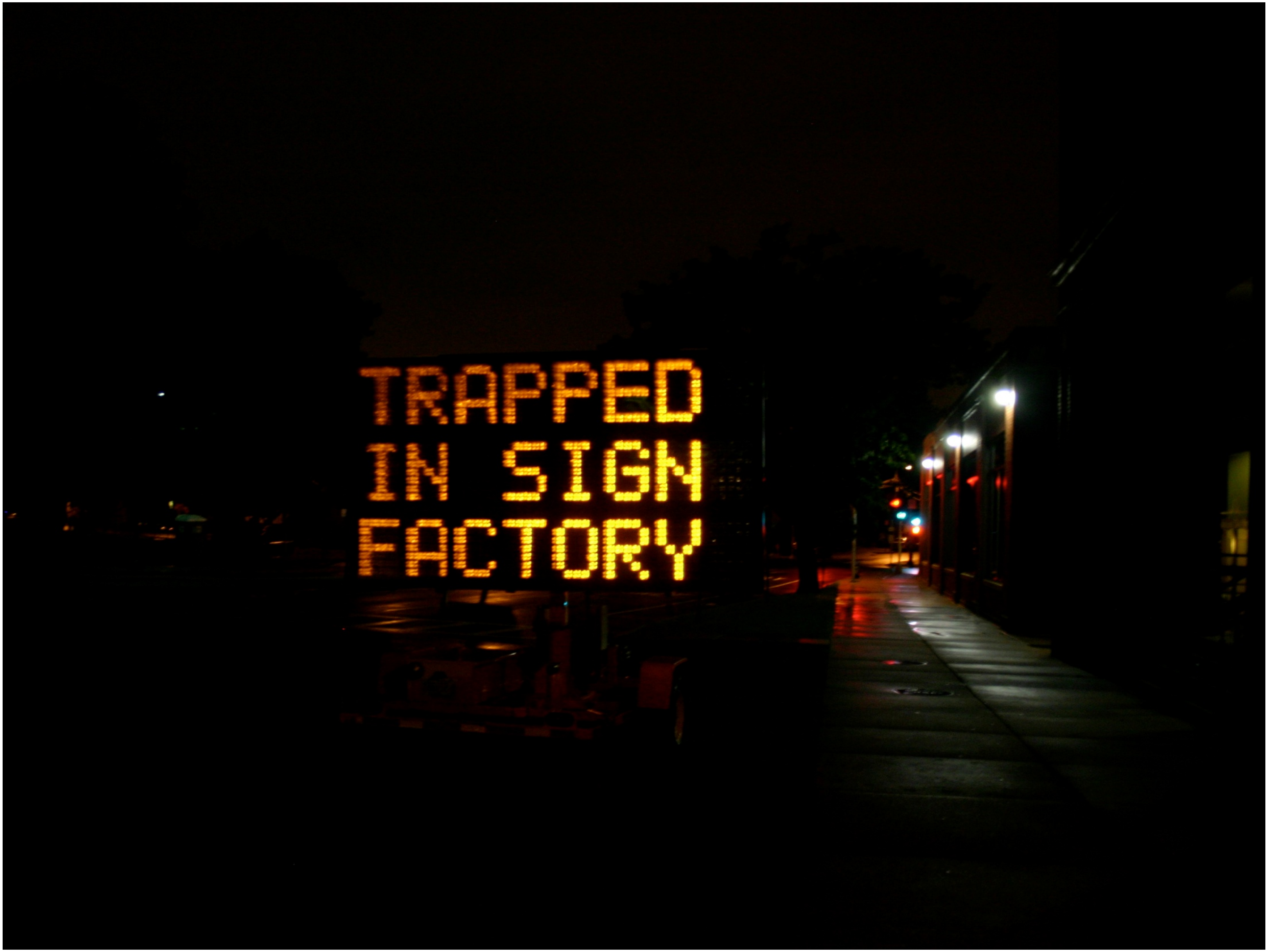
“Design security in from the start.”

ACCIDENT
ON
MOTORWAY
MS.
E
34


ACCIDENT
ON
MOTORWAY
ADMIN
M:29
F1
NO
YES

CAUTION!
ZOMBIES!
AHEAD!!!
RUN FOR
COLD
CLIMATES
THE END
IS NEAR!
!!!!!!!!

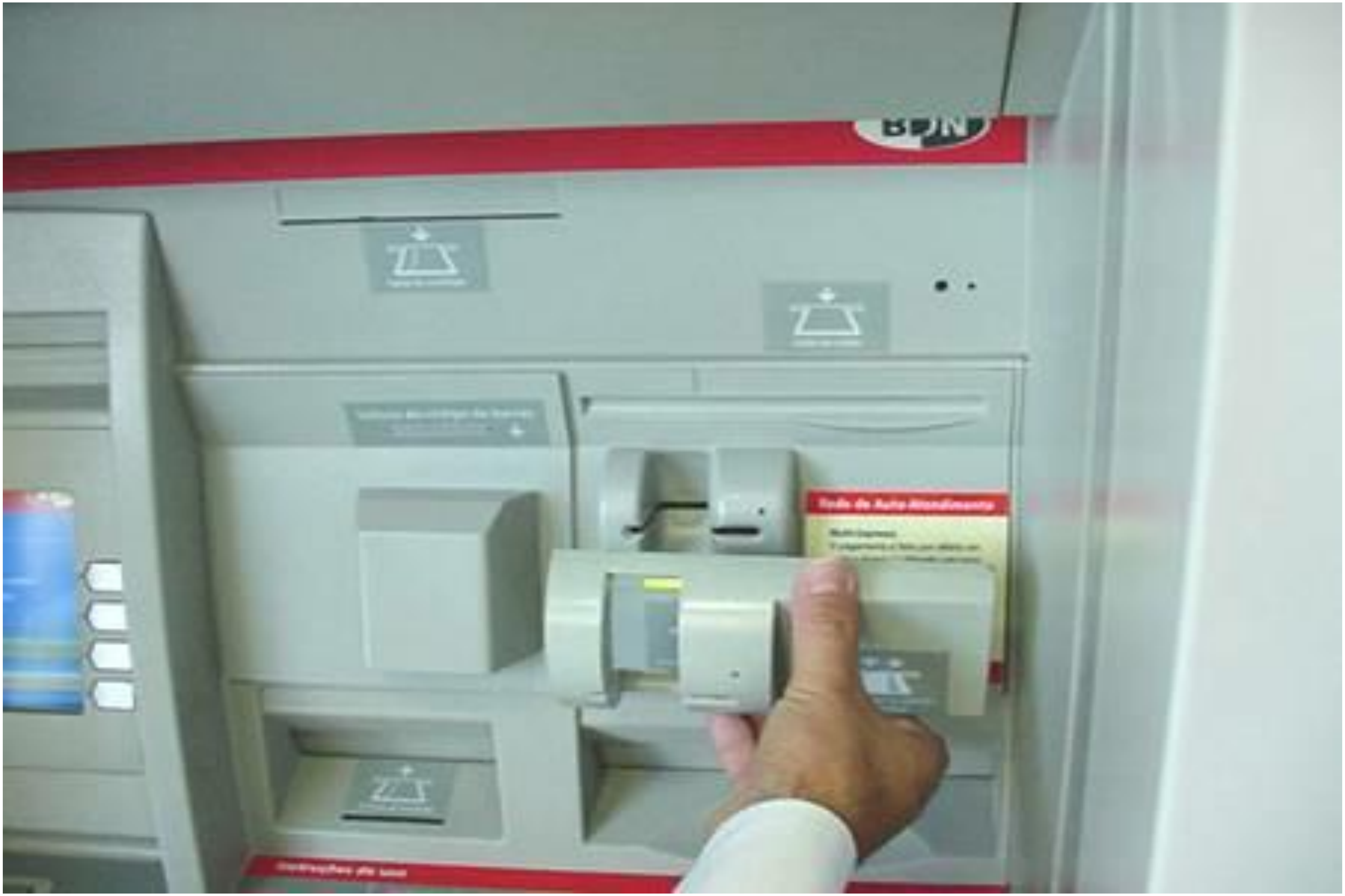
RAPTORS
AHEAD
CAUTION
MARSH


TRAPPED
IN SIGN
FACTORY

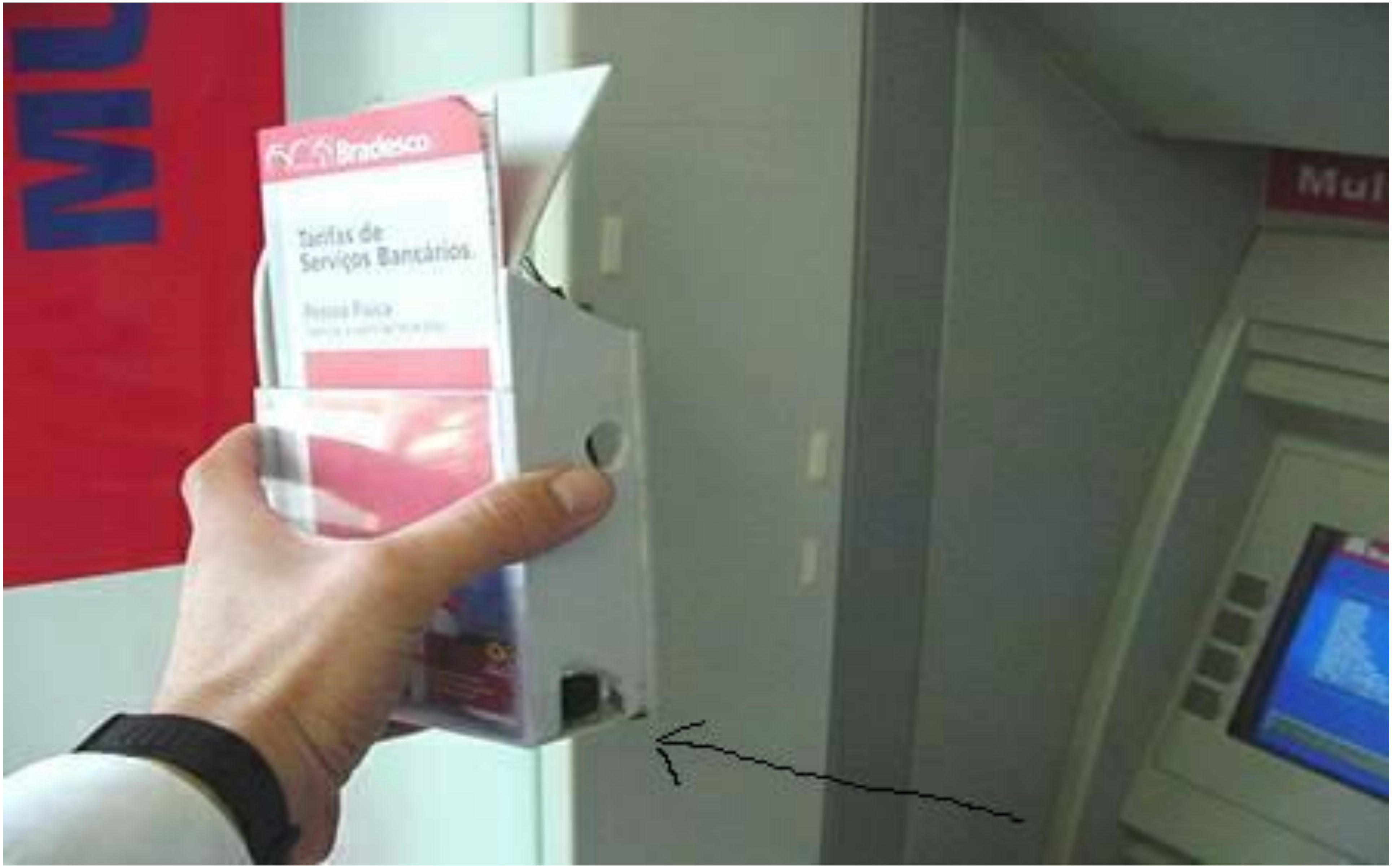
SEND
HELP!

“Don’t rely on security through obscurity.”

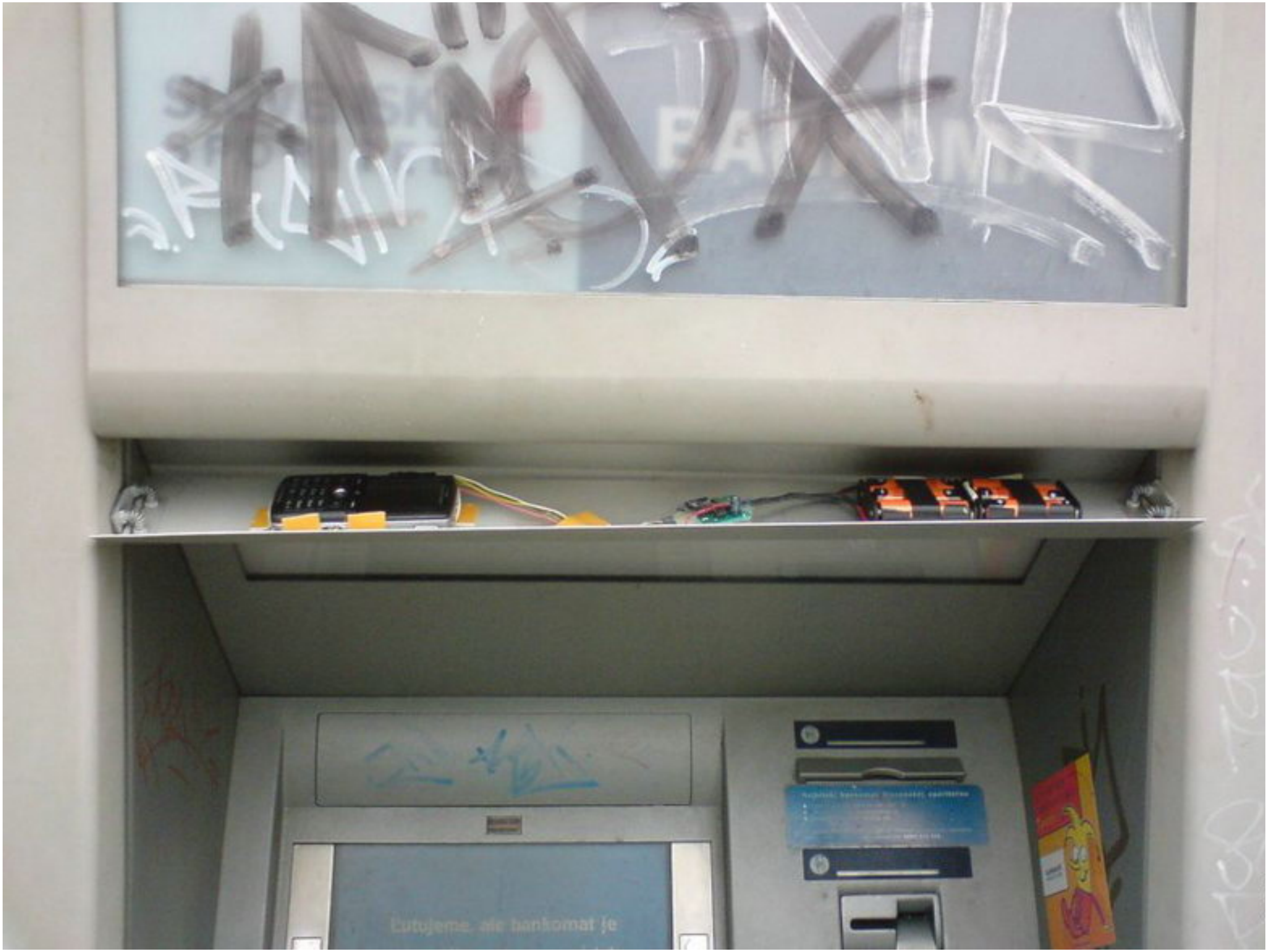
Leitura de código de barras
Bradesco
Instruções de uso


Sala de Auto-Atendimento
Instruções de uso

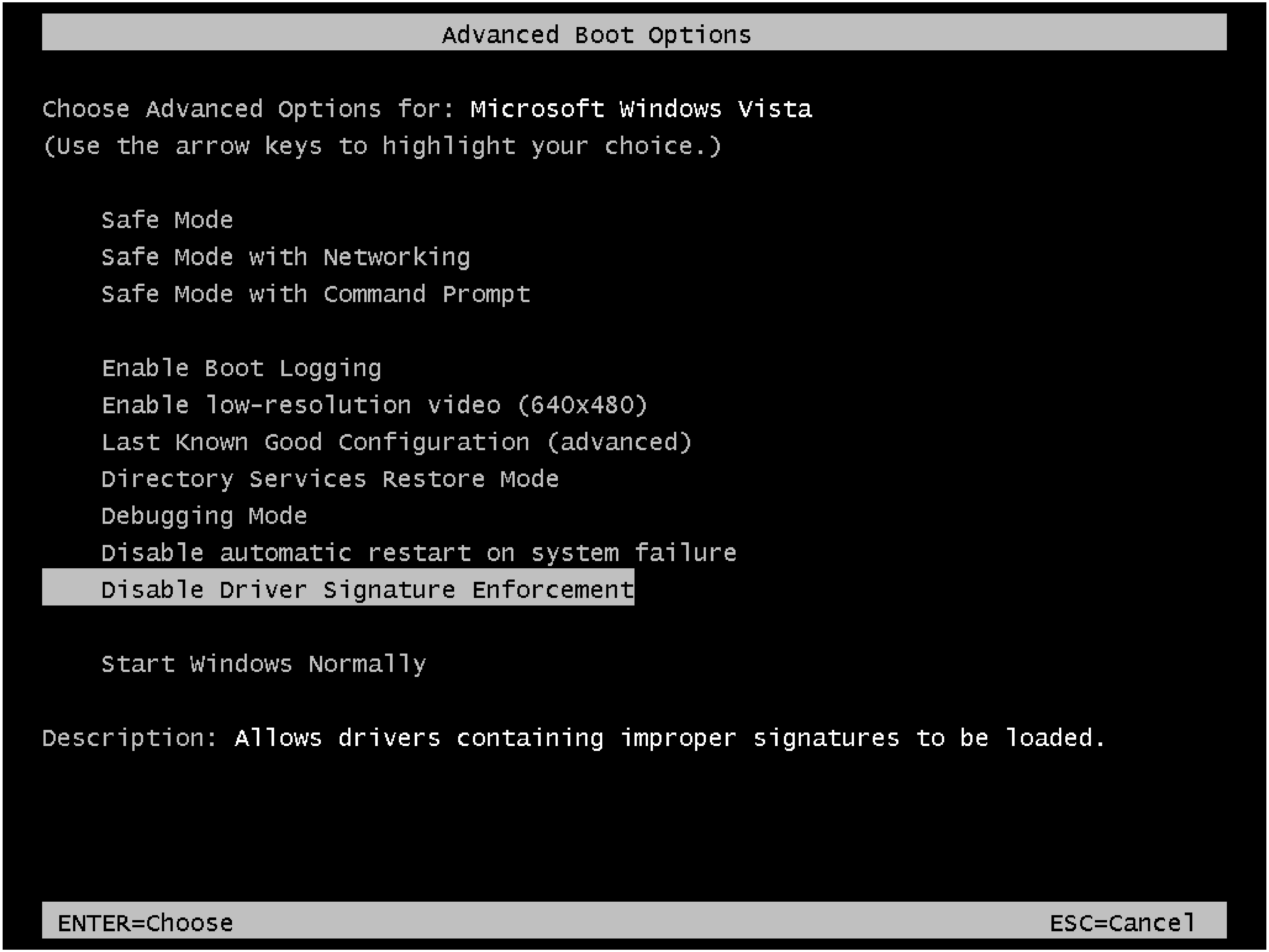
Bradesco
Tarifas de
Serviços Bancários
Pessoa Física
Multi Expresso
Bradesco


MU
Bradesco
Tarifas de Serviços Bancários.
Pessoa Física
Mul

widelec.org
Ľutujeme, ale bankomat je
momentálne mimo prevádzky
We regret this ATM
is temporarily out of service


Ľutujeme, ale bankomat je

“Trusted path.”



```
                              Advanced Boot Options

Choose Advanced Options for: Microsoft Windows Vista
(Use the arrow keys to highlight your choice.)

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video (640x480)
    Last Known Good Configuration (advanced)
    Directory Services Restore Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement

    Start Windows Normally

Description: Allows drivers containing improper signatures to be loaded.




 ENTER=Choose                                                       ESC=Cancel
```

```
procedure withdrawal(w)
   // contact central server to get balance
   1. let b := balance

   2. if b < w, abort

   // contact server to set balance
   3. set balance := b - w

   4. dispense $w to user
```