Workshop on Botnet Detection, Measurement, Disinfection & Defence

Jens Tölle, Fraunhofer FKIE

Botnets

Today and tomorrow, we will see and hear a lot of presentations on botnets and the fight against them.

We will learn a lot about

- policies
- regulatory issues
- responsibilities
- countermeasures

The audience in this room…

In this room here, we are all familiar with the main challenges of botnets.

We understand botnets.

To fight successfully against botnets, we need *a lot of information*:

- technical: software, communication protocols, architectures
- organizational: strategies, business model

… a lot of information!

- reverse engineering….

  ….to try to understand protocol interactions

- distinguish bot communication from “clean” traffic

- breaking cryptography….

  …to see what the bots are talking with each other

- understanding c&c architecture….

  ….to understand who and where the boss is

- analyzing bits and bytes!

… a lot of information!

That‘s a job for experts

Experts need to understand what‘s going on.

Experts need *Situational Awareness.*

Situational Awareness?

but…

Computer user

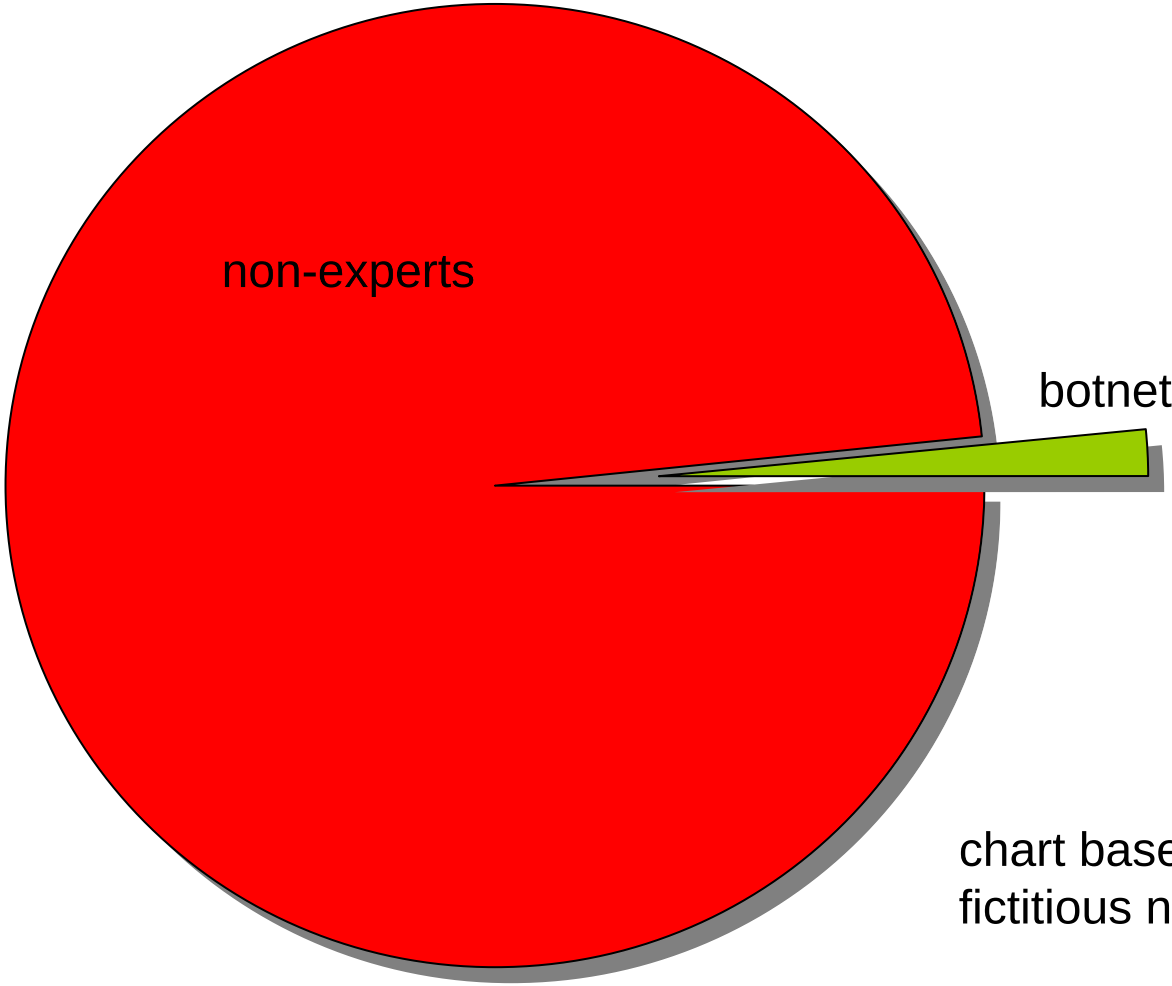


chart based on
fictitious numbers…

Botnet sustainer

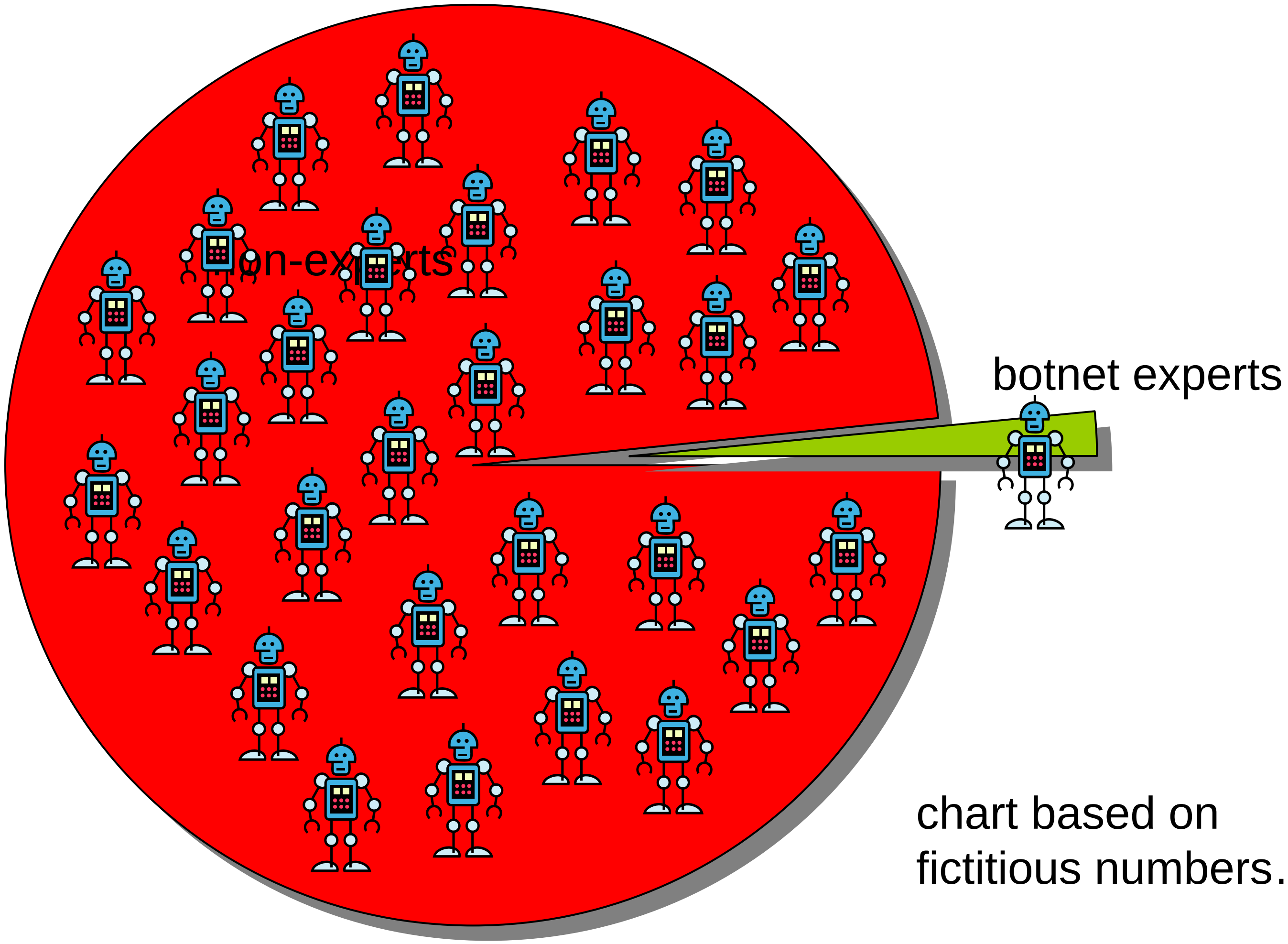
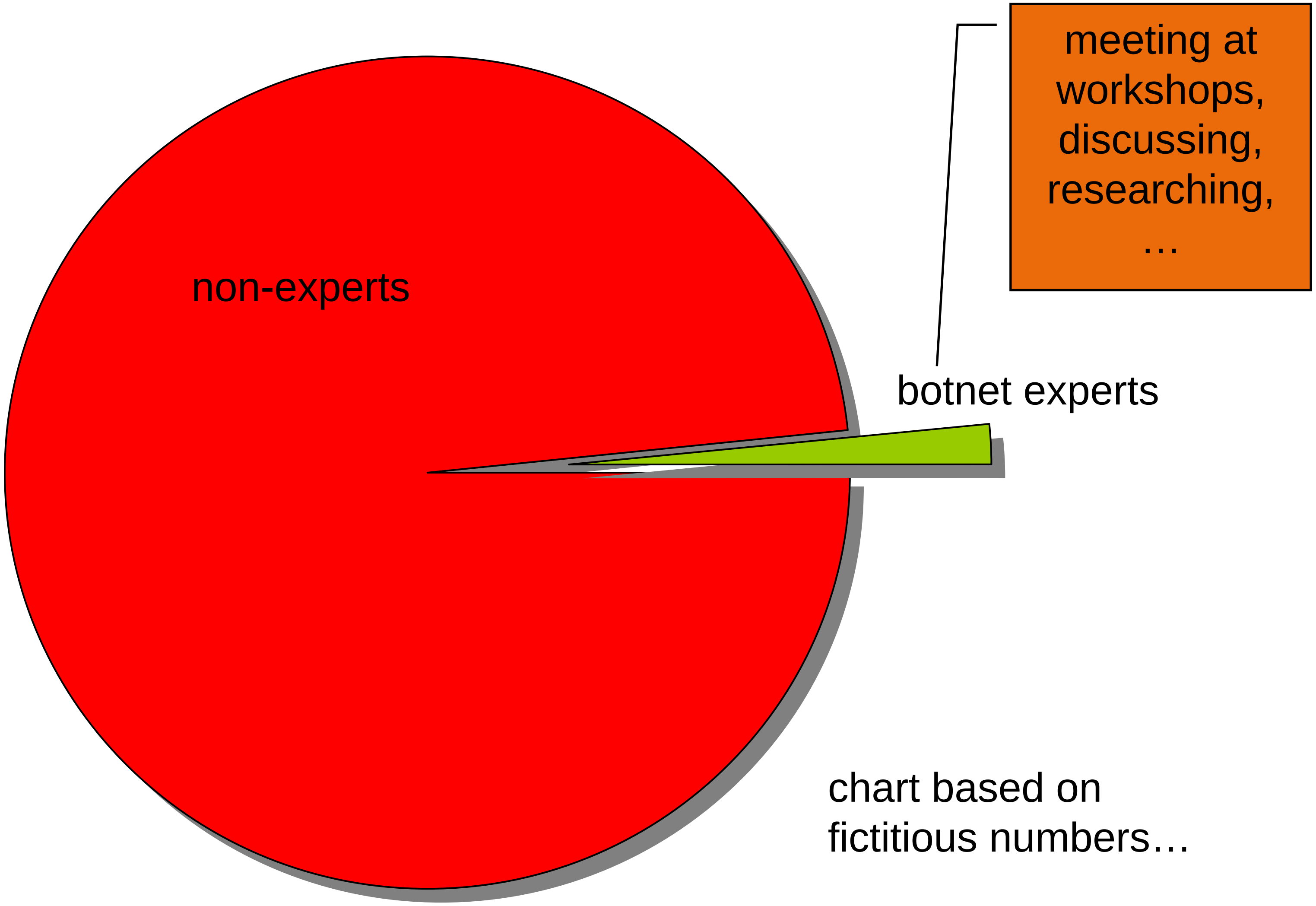


chart based on
fictitious numbers…

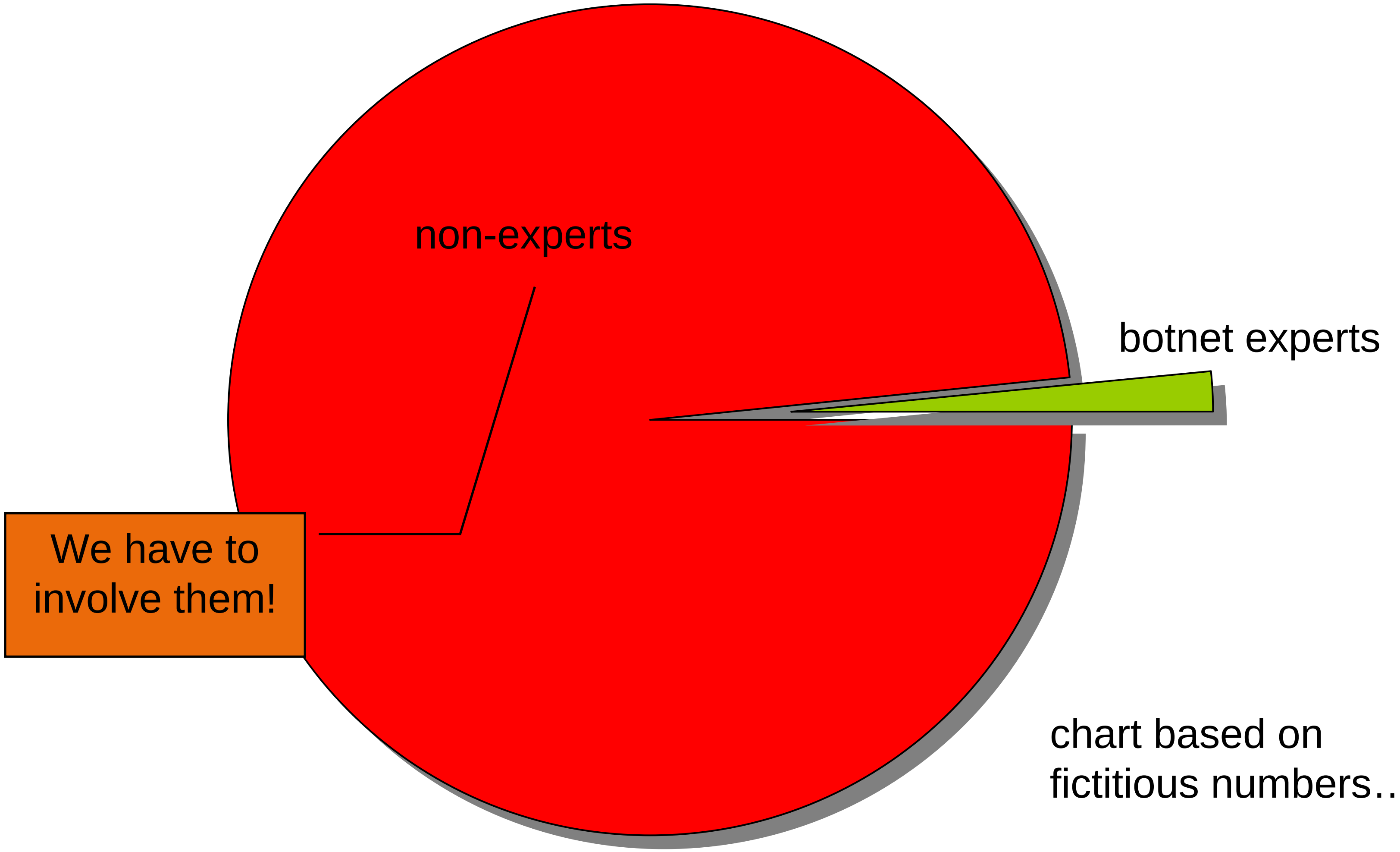
What to do?



meeting at workshops, discussing, researching, …

chart based on fictitious numbers…

And what else?



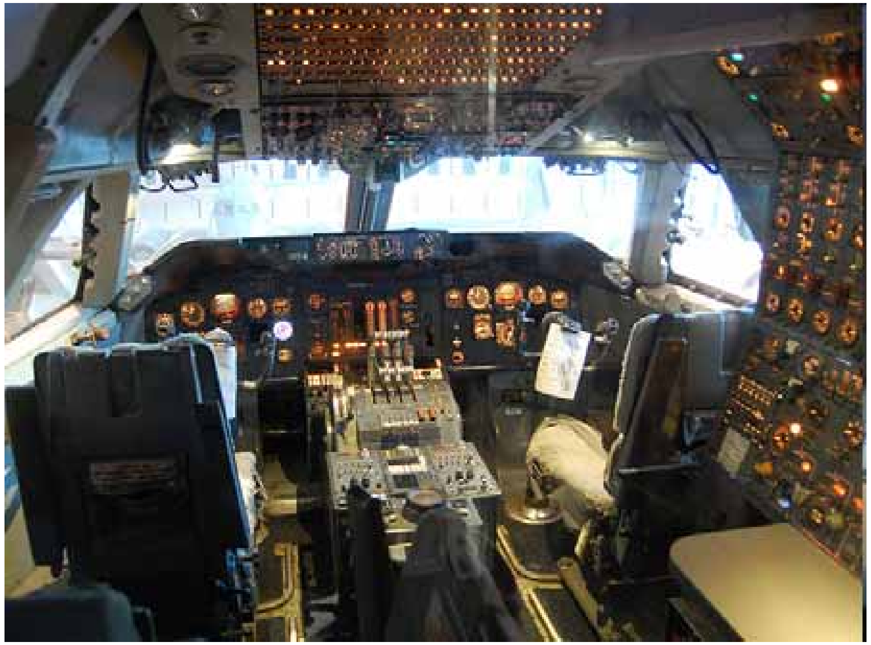
We have to involve them!

chart based on fictitious numbers…

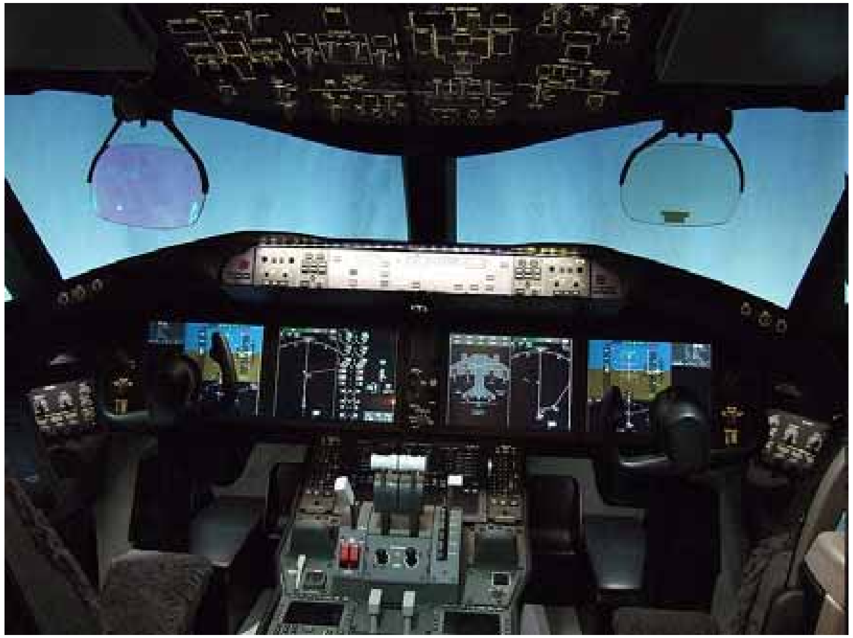
How?

How can we involve the non-experts?

First idea: Make things simpler....



Boeing 747-100



Boeing 787

But this is still for experts...

http://commons.wikimedia.org/wiki/File:747-100_Cockpit.jpg

User: Fletcher6, License CC BY-SA 3.0

http://commons.wikimedia.org/wiki/File:787-flight-deck.jpg

License PD

Let‘s take something simpler…

Operating a plane is a complex task… …and pilots are experts.

Operating a car is definitely easier… …does it require experts?

What we can learn from cars…

Cars are complex

They may suffer from different problems

It‘s not easy operating them

They may be dangerous to others

Computers are complex

They may suffer from different problems

It‘s not easy operating them

They may be dangerous to others

What we can learn from cars…

Operating a car is a complex task

People are aware of this…

…and they understand and accept it.

People need a driver‘s license

Operating a computer is a complex task

People are aware of this…

…but it‘s the computer‘s fault

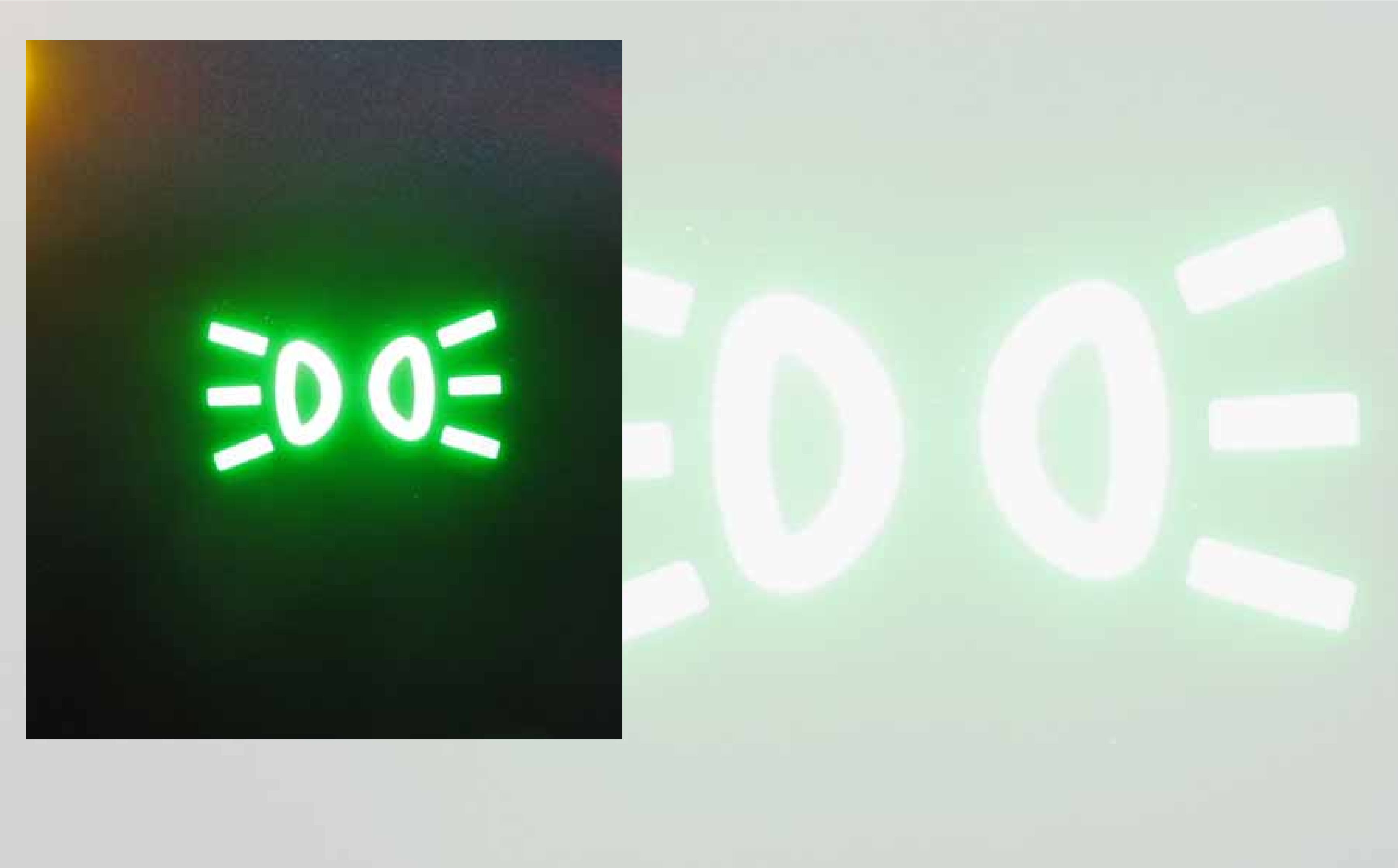
People do not need a *computing license*

People don‘t care

Give people the amount of information they need…

…and not more!

Green means ‘ok’…



Orange means ‘pay attention‘

Red means ‘danger‘

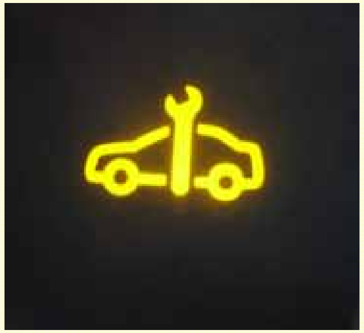
And what about computers?

Installing software is often complicated and confusing.

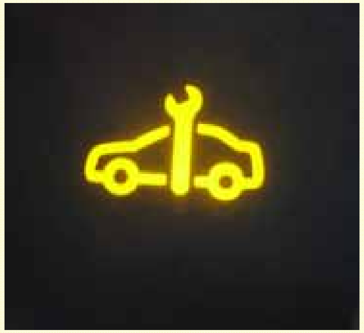
Configuring applications, e.g. anti-virus software, is not easy.

Reading and understanding message windows seems to overstrain a lot of users.

But these people generally understand this:



They know what to do, when they see this!



They do not know exactly what‘s wrong. And they do not have to know!

They ask someone who knows. They go and see their repair shop.

Emergency operation

Sometimes a car refuses to start in order to prevent further damage.

Sometimes a car offers a basic emergency operation (without full performance, but protecting the user, the car and others).

An Internet provider will hesitate to interrupt one‘s connectivity in case of malware problems (warranty, liability, service level agreement, communication in cases of emergency…)

But is some kind of „emergency operation“ possible?

More than an indicator light?

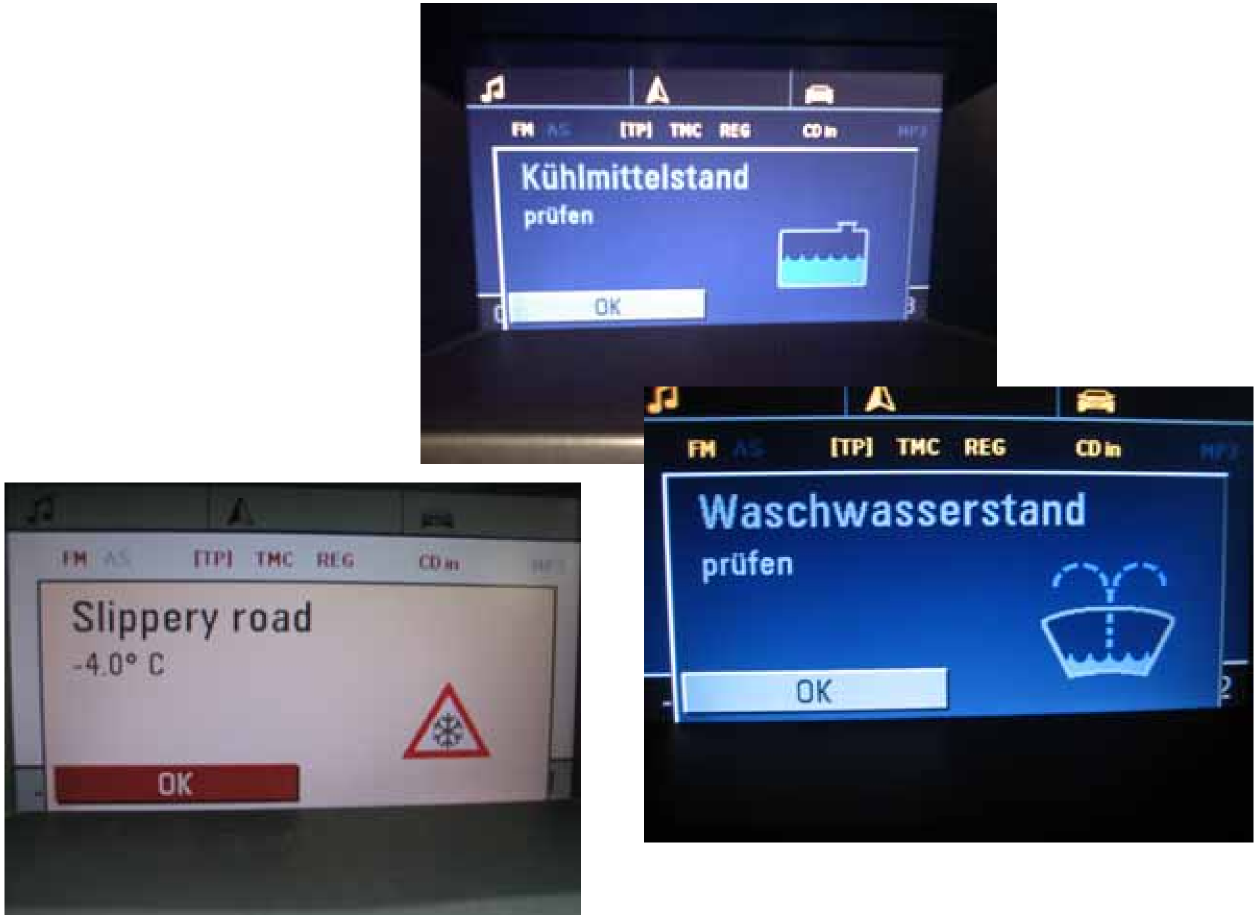
If you really want to give a user more information than

consider the following points:

- Can the average user understand the message?
- Is the message simple enough?
- Does the user know what to do?

If you are not sure, than don't do it!

Tell a user what to do…



Kühlmittelstand
prüfen

Waschwasserstand
prüfen

Slippery road
-4.0° C

…and keep the message simple!

Take-home message

Do not forget the non-expert users!

It‘s their systems where the bots are.

They are no experts – and they will never be.

They just want to use their computers.

So make it simple.