Circumvention is not privacy!

aka
The Hitchhiker's Cautionary Tale of a Social Revolution in 10'

nds@it46.se

What you do not see, can hurt you!

Internet and other communication networks can be controlled by three basic technical mechanisms:

- Filtering
- Interception
- Tampering

The problem

- Major efforts has concentrated in bypassing filtering, blocking i.e. circumvention.
- Access to the network has been blindly promoted at the expense of personal safety.
- Centralized and close solutions promoted as revolutionary (social networks) are in fact dual-use technologies.
- The potential for change of Internet remains largely unexploited.

Always in a hurry!

- Tools are given more importance than strategies
- Infrastructure is supported by identification through advertisement
- The new "mantras" of Internet: Freedom, net-activisms, hacktivism
- Risk analysis are largely ignored
- Traditional institutions want to embrace activism without understanding its (core) values

Fast and furious

“Do you have one minute? We have a revolution going on now in Egypt, can you tell me quickly how we connect to the Internet?”

“Can you provide us a training in secure communications? Can we do it in one-day?

Information wants to be free in an non-free infrastructure

"Our website is under attack? Can you protect the site right now?

It is too expensive we are getting free-hosting at the moment. We can not pay!

Approach to circumvention tools in "challenging areas"

- Ten tools analyzed including: dynaweb, ultrasurf, tor, freegate, gtunnel, JAP, yourfreedom, phisphon,...
- Outcome 1: A methodology to address tools i.e. trying to compare apples and oranges
- Outcome 2: A lab environment to reverse engineer tools
- Outcome 3: Ten recommendations

Outcome 1 (Evaluation Criteria)

I am with S.T.U.P.ID

Sustainability

Trust

Usability

Privacy

Infrastructure Development

Outcome 2 (Evaluation Methods)

Infrastructure for analysis

- Laboratory environment
- Reverse engineer methods
- Security, Privacy
- Resistance to DDoS attacks
- Check list and tests
- Metrics for evaluation

Outcome 3 (Recommendations)

- **S**ustainability of circumvention solutions:
  - Can only be achieved by long term support models
  - Can not rely in per-country approaches
- **T**rust requires:
  - Peer review of code and system implementations
  - Openness, addressing limitations and risk analysis

Outcome 3 (Recommendations)

- **U**sability:
  - Should not only focus in functionality but educating the users about the decisions they are making
  - Requires all types of training adapted to the beneficiaries
- **P**rivacy:
  - Larger research investments are needed in making tools and traffic untraceable/unobservable. Obfuscation by default!
  - Users need to be better informed about what Personal Identifiable Information is involved in the usage if a tool.

Outcome 3 (Recommendations)

- **I**nfrastructure **D**evelopment:
  - Further investments are needed in decentralized and peer-to-peer models.
  - Human infrastructure are the ultimate tools.

NDS

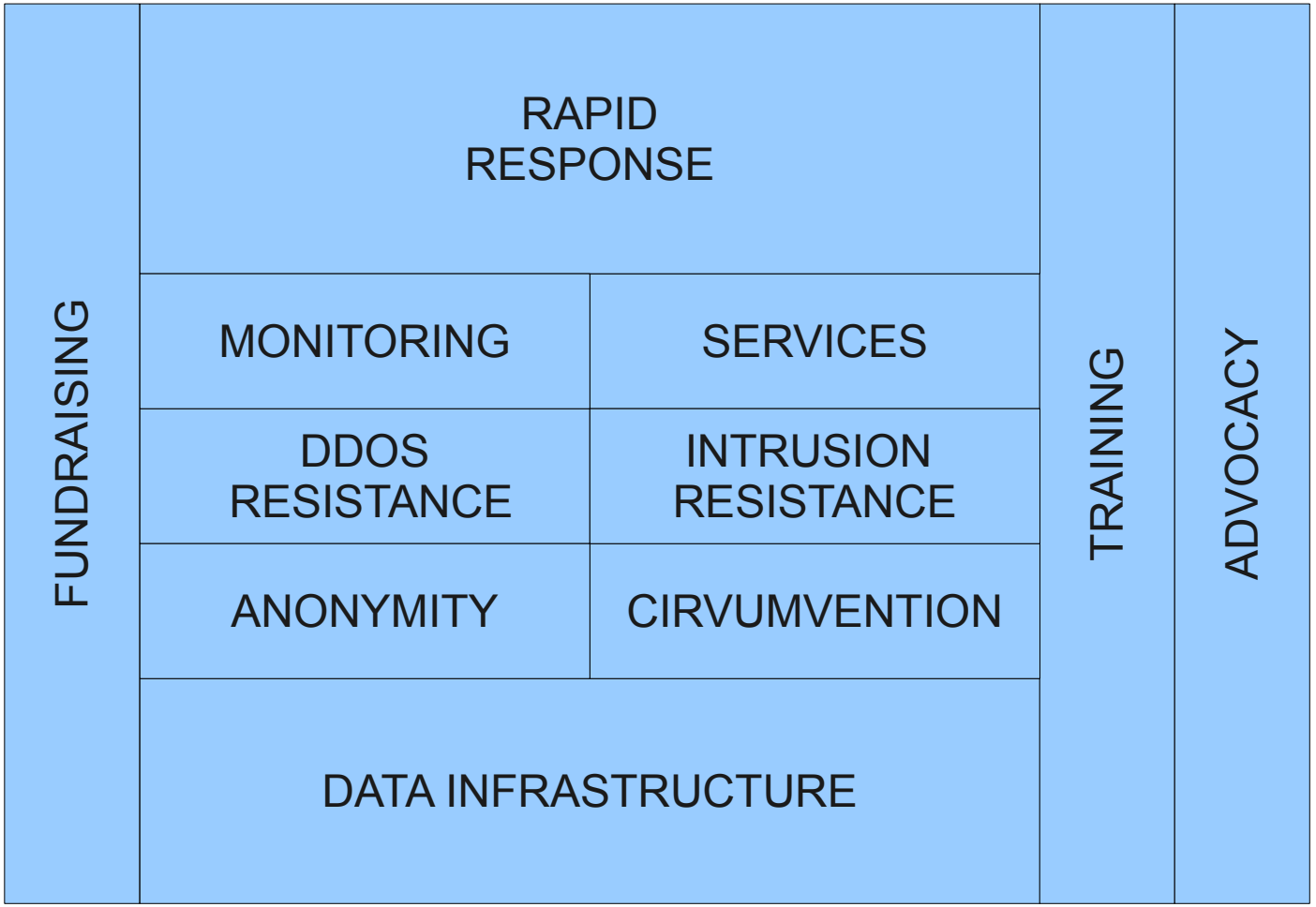
It aims at providing citizens living in non-democratic regimes with the **technological tools** they need to shield them from **indiscriminate** surveillance or bypass **disproportionate** restrictions on their freedom to communicate.

NDS

It aims at providing citizens
with the **tools**
to communicate.

+ safely

Safe Connection Strategy




MACBEAST