Rock Solid Internet Exchange

Nätangrepp mot Sverige

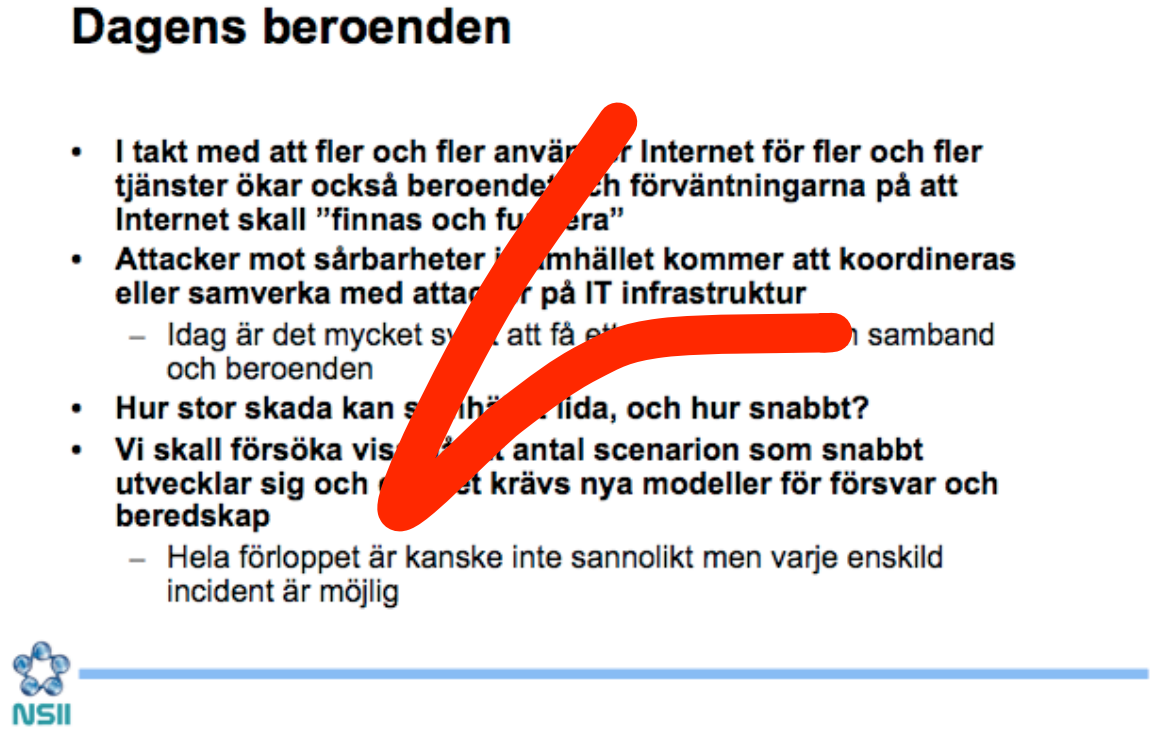
NETNOD

Rock Solid Internet Exchange

TOLD YOU SO!

NETNOD

Internetdagarna 2006



Attacks against a state based on activism

NETNOD

Rock Solid Internet Exchange

Internetdagarna 2006

NETNOD

Rock Solid Internet Exchange

Our "own version"

Lessons learned from Estonia

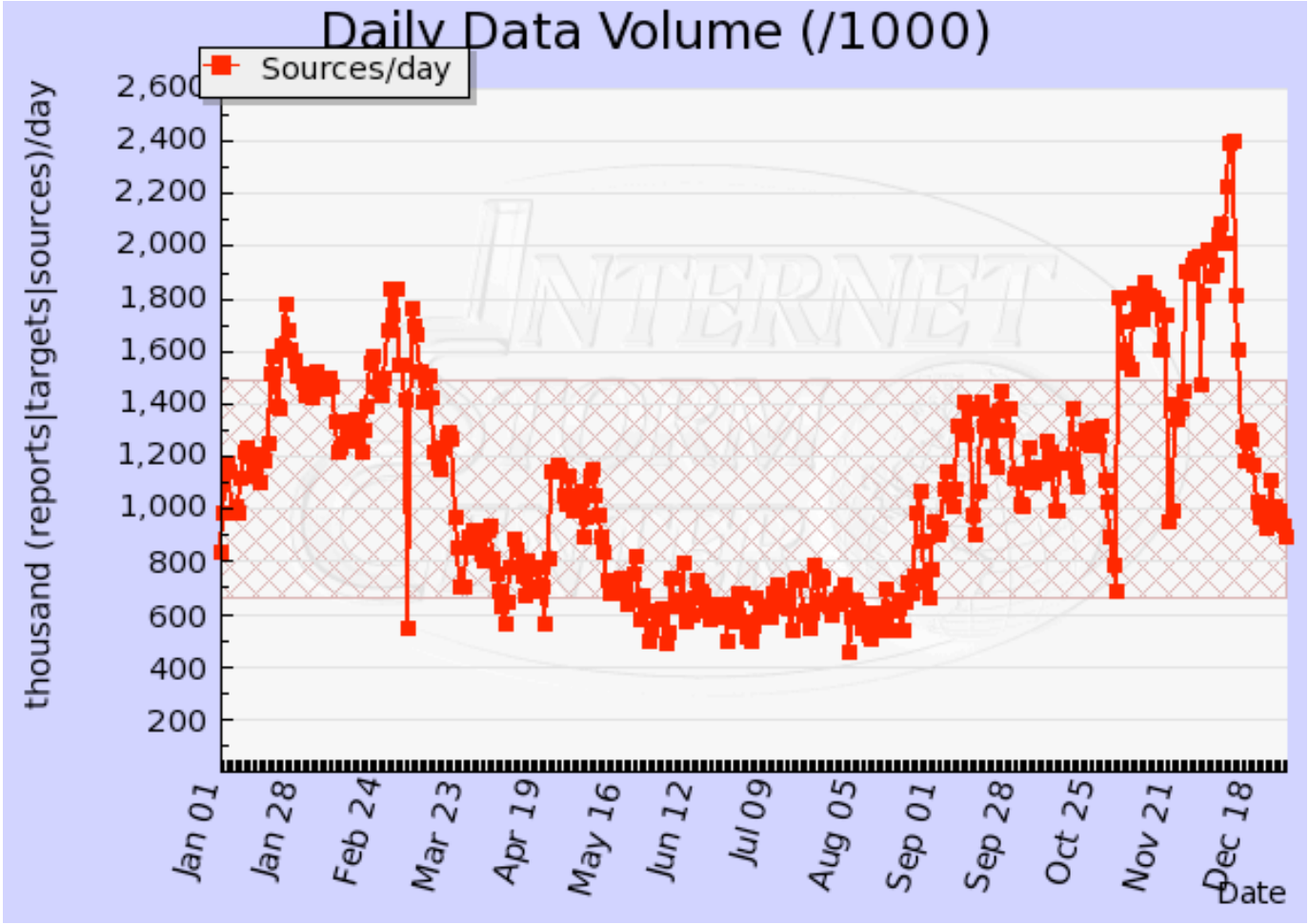
- We actually had 6 months head start...
  - ...or could have had
- The attacks on Estonia where not unique
  - Similar attacks against NATO during the campaigns in Serbia etc.
  - So they are likely to happen again

So what happened in the mean time..

- Here? Not much...
- In the rest of the word on the other hand...

Rock Solid Internet Exchange

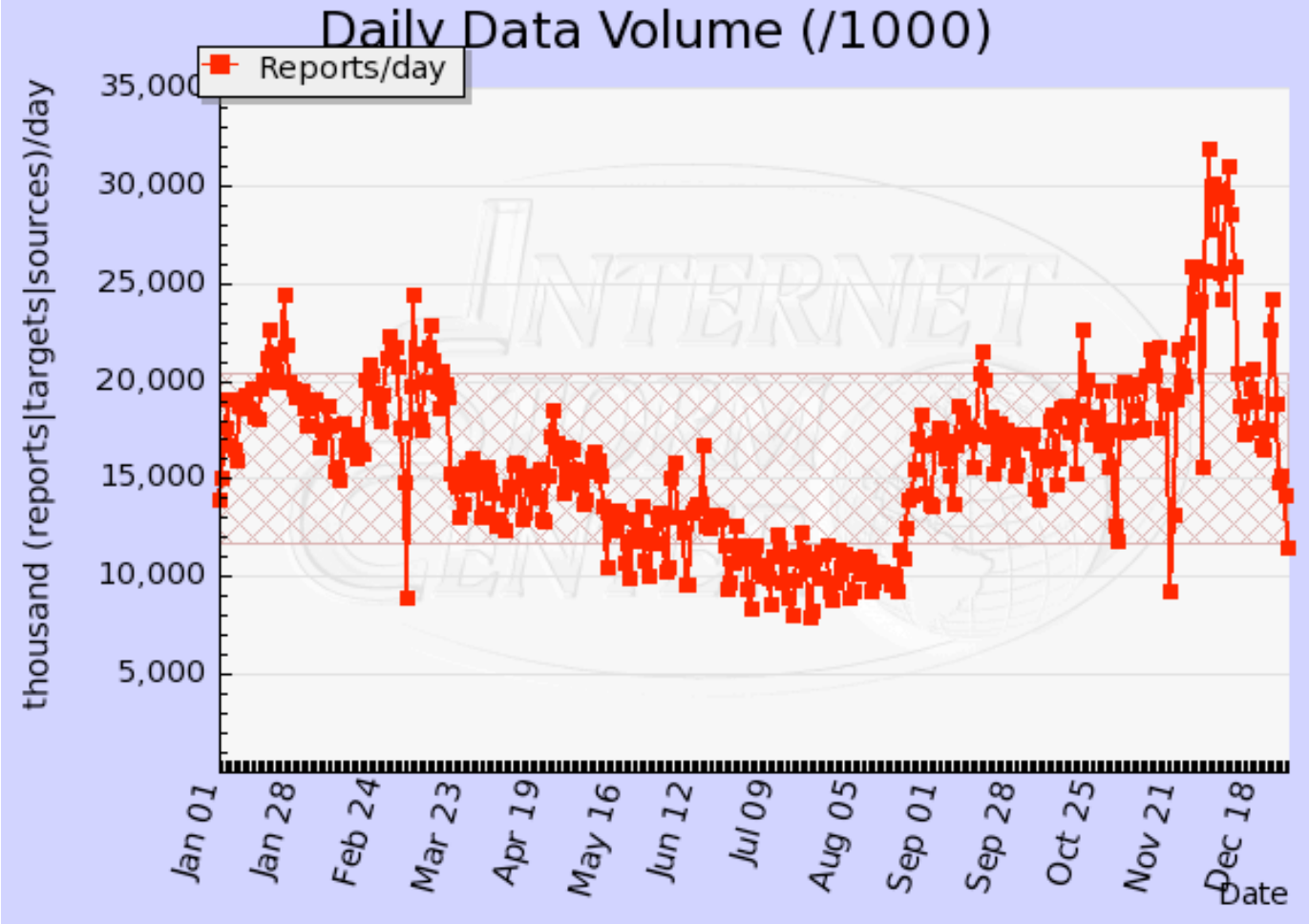
SANS sources / day report



NETNOD

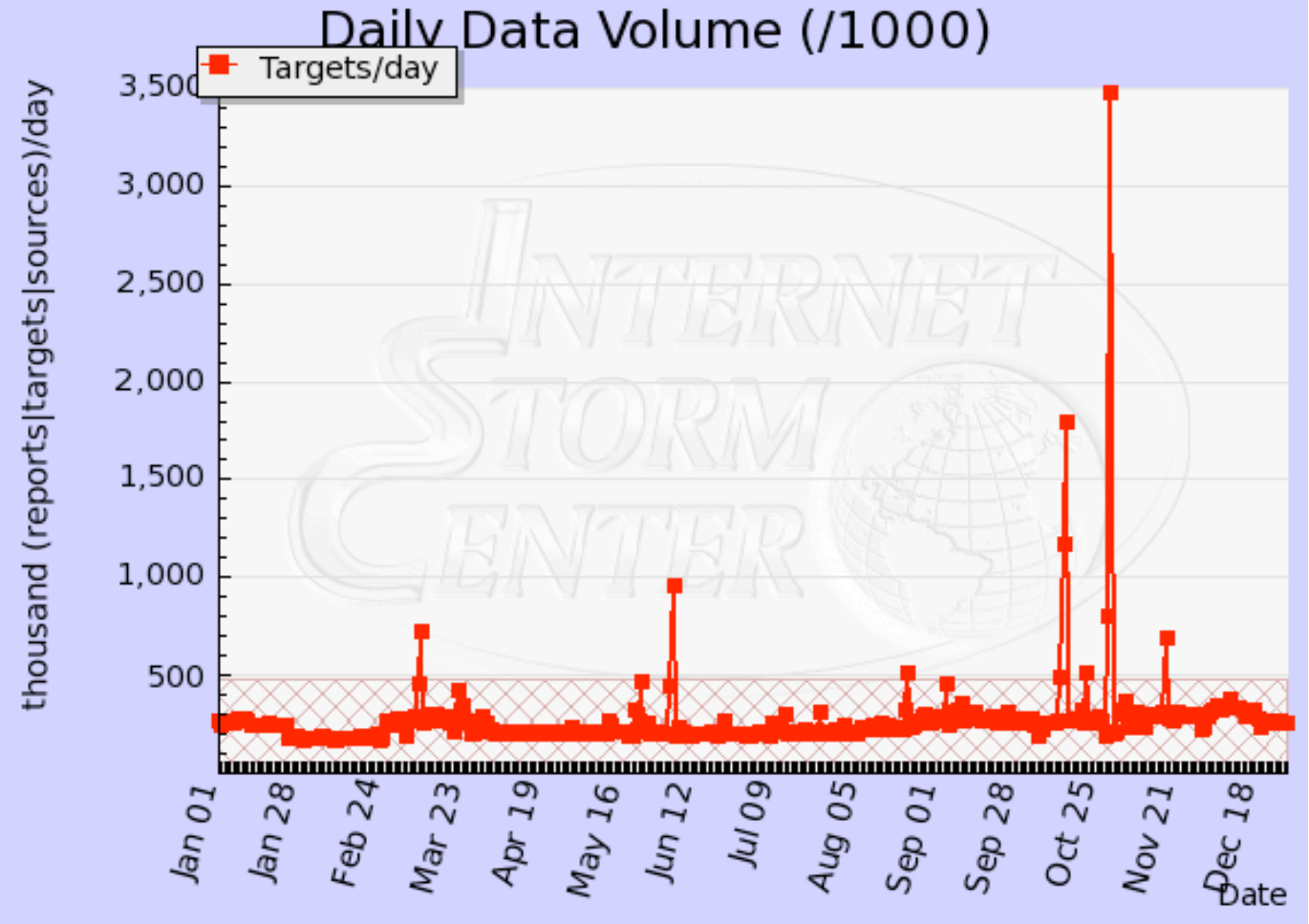
Rock Solid Internet Exchange

SANS reports /day report



NETNOD

SANS targets / day report



Country	Region	Reports
	All	
UNITED STATES	NA	1,025,437
CHINA	AS	845,749
GERMANY	EU	281,602
ITALY	EU	239,762
TAIWAN	AS	167,701
AUSTRALIA	AU	157,434
CANADA	NA	145,477
AUSTRIA	EU	117,625
JAPAN	AS	99,198
BRAZIL	SA	91,041
NEW ZEALAND	AU	80,127
KOREA, REPUBLIC OF	AS	75,861
FRANCE	EU	73,036
UNITED KINGDOM	EU	57,903
SWITZERLAND	EU	56,495
THAILAND	AS	53,457
SWEDEN	EU	51,625
SPAIN	EU	47,853
RUSSIAN FEDERATION	EU	35,538
POLAND	EU	33,654
INDIA	AS	30,644

- FTTx in Asia grew with 20% per Q in 2006

Now what?

- We lost 12 important months
- In the mean time the potential attack capability grew
- We still have no or little means of coordinated protection
  - And we don't even know *what* to protect...

Lessons learned from Estonia

- Even if the attacks where not unique they where somewhat odd
  - These attacks where not done for economic gain - they where based on ideology
  - They where more or less co-ordinated
  - They where not directed against homogenous targets other than a country

How do you handle this?

- Described in my presentation at last years Internetdagarna conference
- Although several discussions with authorities nothing happens
  - But there are more studies being conducted
  - Oh, and they visited Estonia
- Sweden is today as vulnerable as a year ago
- We could have had a year of preventive work behind us...

More we could have done...

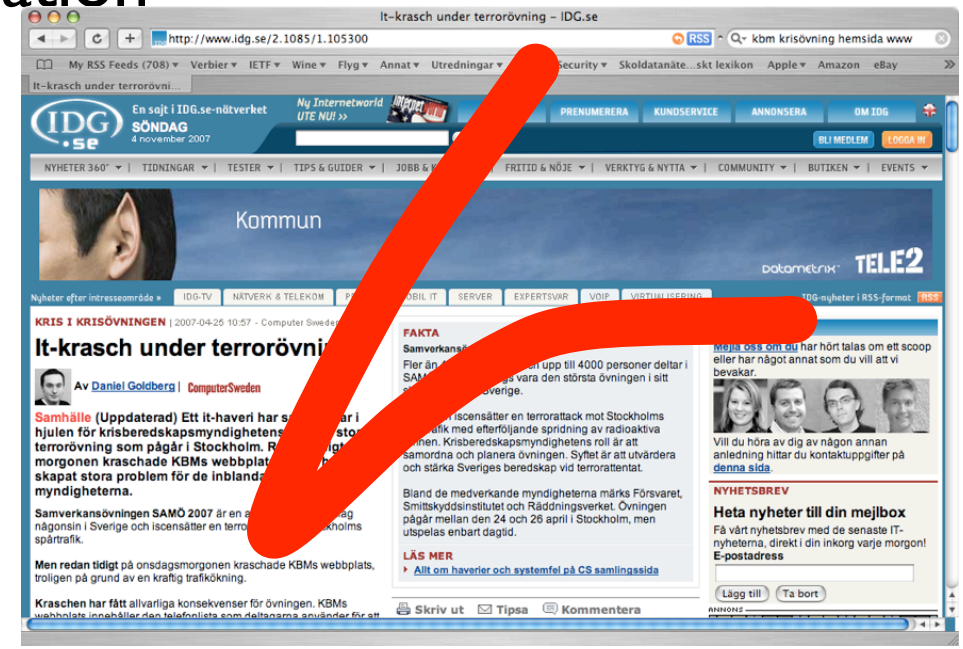
- Most agencies today are still single homed
- How do they communicate in terms of crisis?
- How do I communicate with them in terms of crisis?
- Who do I communicate with in terms of crisis?
- Who do I think I am communicating with in terms of crisis?

Trends

- Attacks are generally conducted for economic gains
- Short of this we are seeing new types of attacks that (potentially) are of national concerns
  - Hacktivism aka what we are already observing
  - “Forced information leakage attacks” and ensuing trading in information
  - Government sponsored, targeted attacks

What can/should we do?

- I already last year pointed out the need for a government authoritative service that citizens can trust and turn to for accurate information



What can/should we do?

- The Estonians had an advantage in that all government connections was handled by a competent, centralised group that had authority to act
  - And had operational data and knowledge
- Today you have two problems
  - Detecting the attack
  - Mitigating the attack

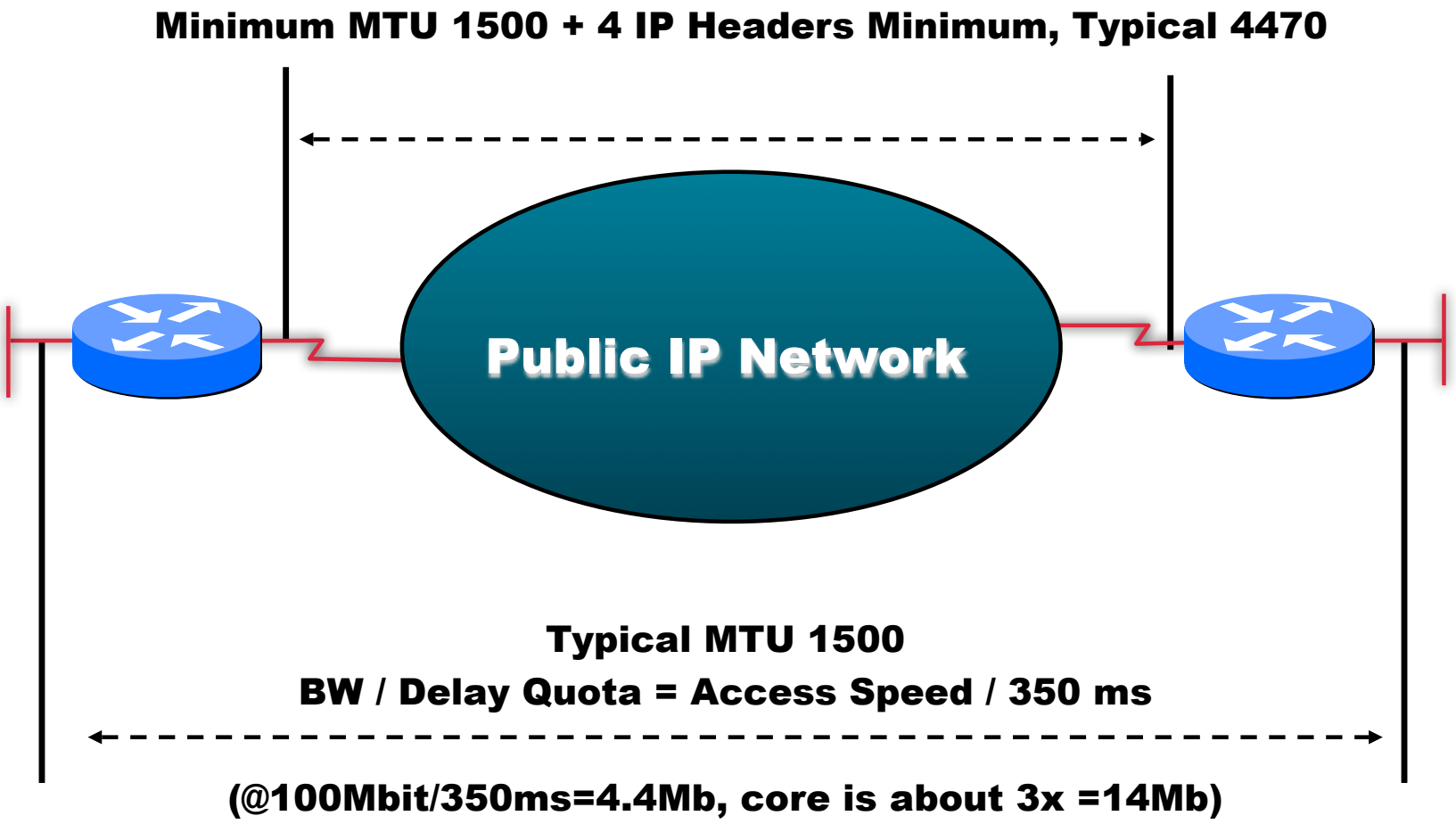
Detecting attacks

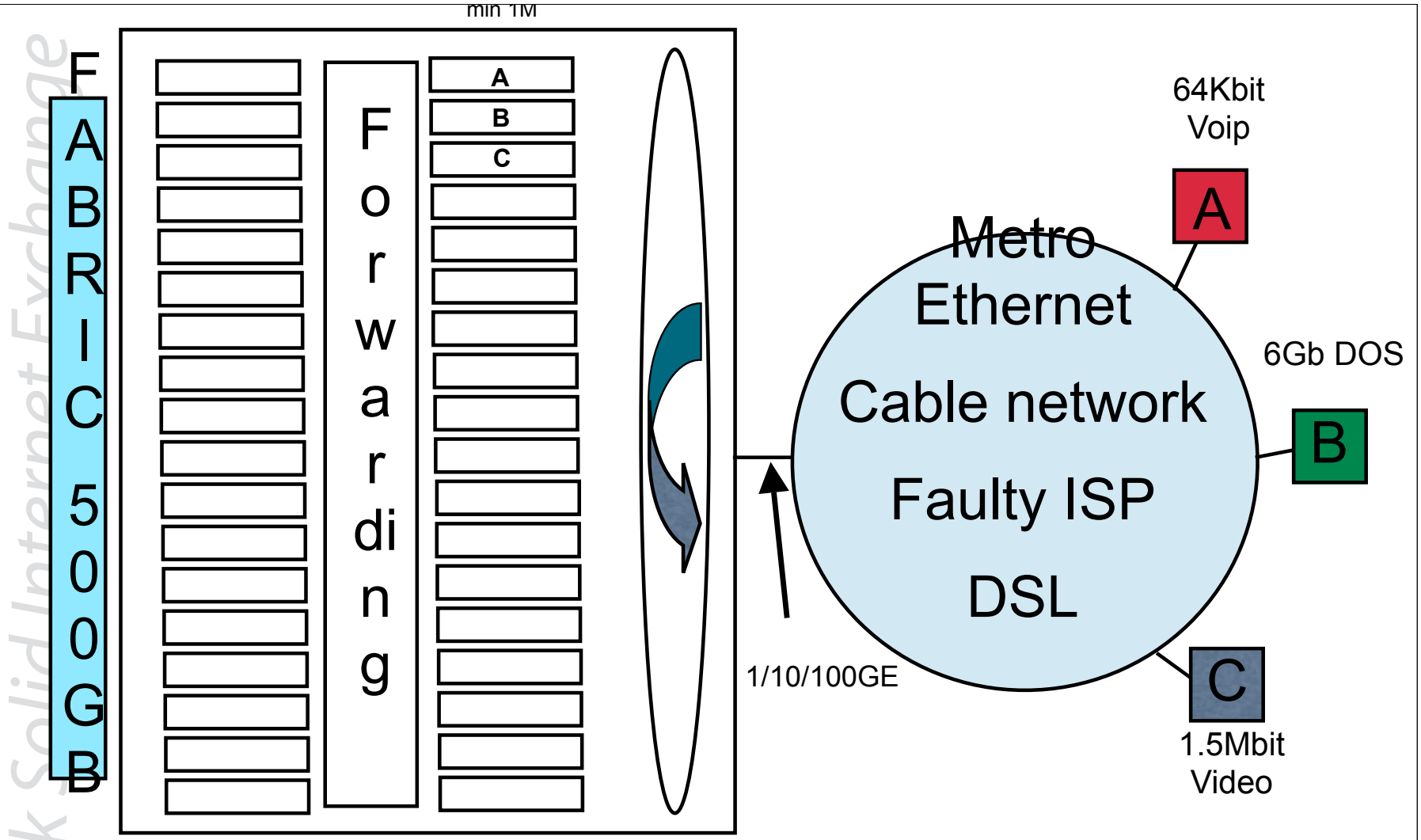
- DDOS
  - Could be hard to distinguish from a KBM exercise or the release of the new budget...
- Tailored virus attacks
  - How do you know what documents/mails are leaking?
- Prefix hijacking
  - How do you track who announces what?

Mitigating attacks

- DDOS attacks
  - You need to look into the IP packet before you can drop
  - Routers are targeted at forwarding packets fast - not reading them fast
- Tailored viruses
  - Should be simple :-) But see above...
- Prefix hijacking
  - Needs operational skills - but there are commercial services....

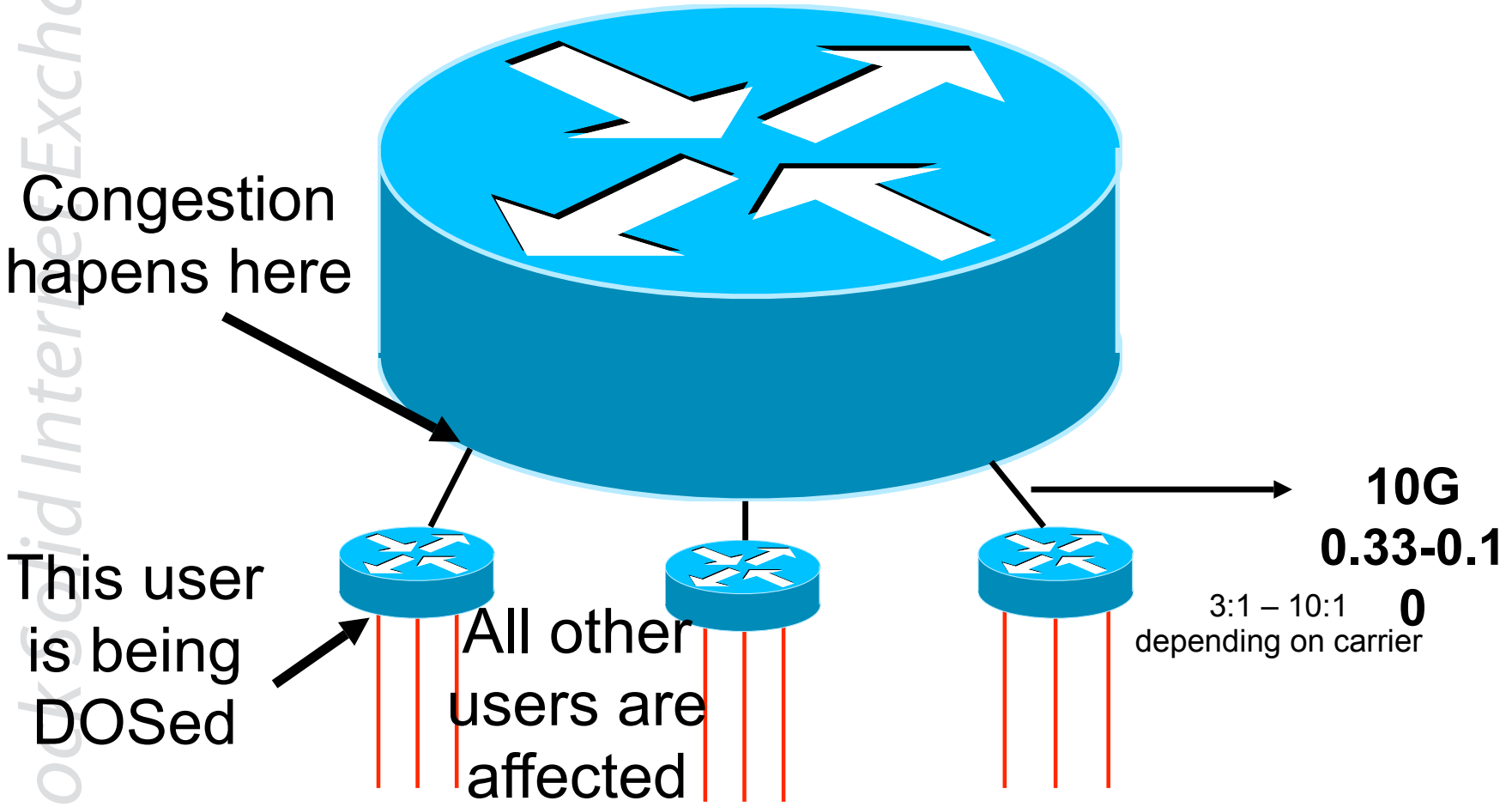
The Net



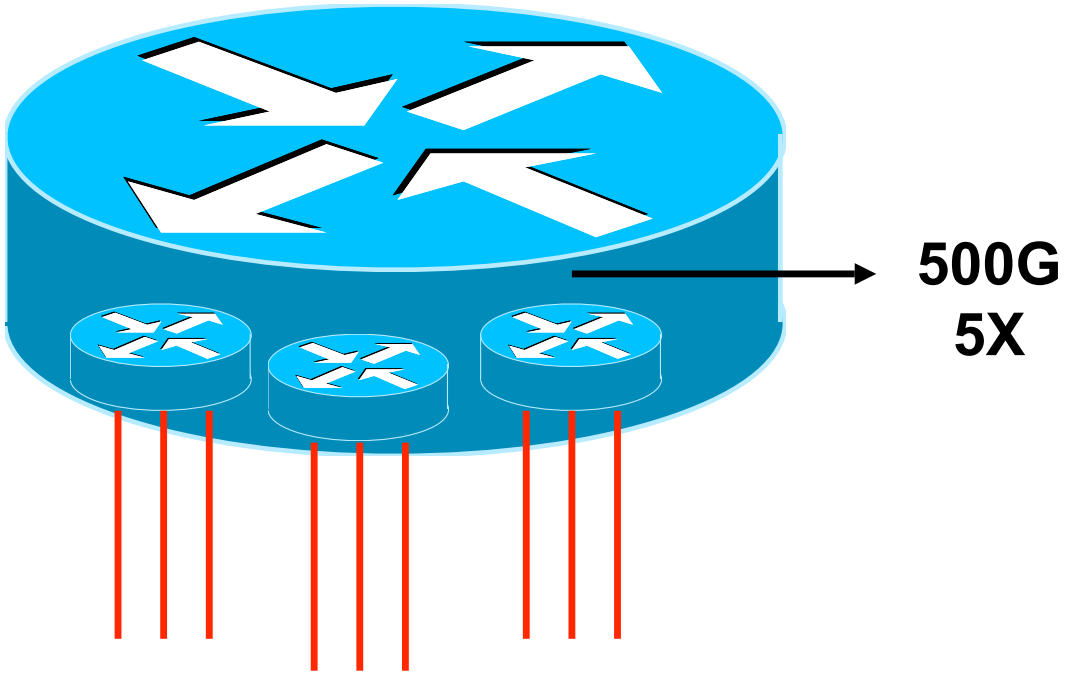


The upstream router has to look at packets 5-7 times faster than an output interface. Drop the unwanted traffic and queue and shape for the no_buffer oversubscribed network

A common way to build a IP POP
Oversubscribe the edge boxes



One way to solve the problem is to integrate core and edge, but we need edge forwarding engines that runs at 5-7X



TODO list for next year

- Require agencies to have a minimal of correctness in their Internetaccess
- Decide who is responsible for communicating to the citizens in terms of crisis
  - Build a scalable, distributed system that can be reached at all times, and that is operated within the day-to-day infrastructure
  - For example anycast from the PTS bunkers / IXes etc

TODO list for next year

- Analyse the need for communications between the government agencies
- Study external dependencies
  - We are not as fortunate as Estonia due to Oxelstierna. Agencies are autonomous
- This is engineering. Build within normal operations - but build it good

Rock Solid Internet Exchange