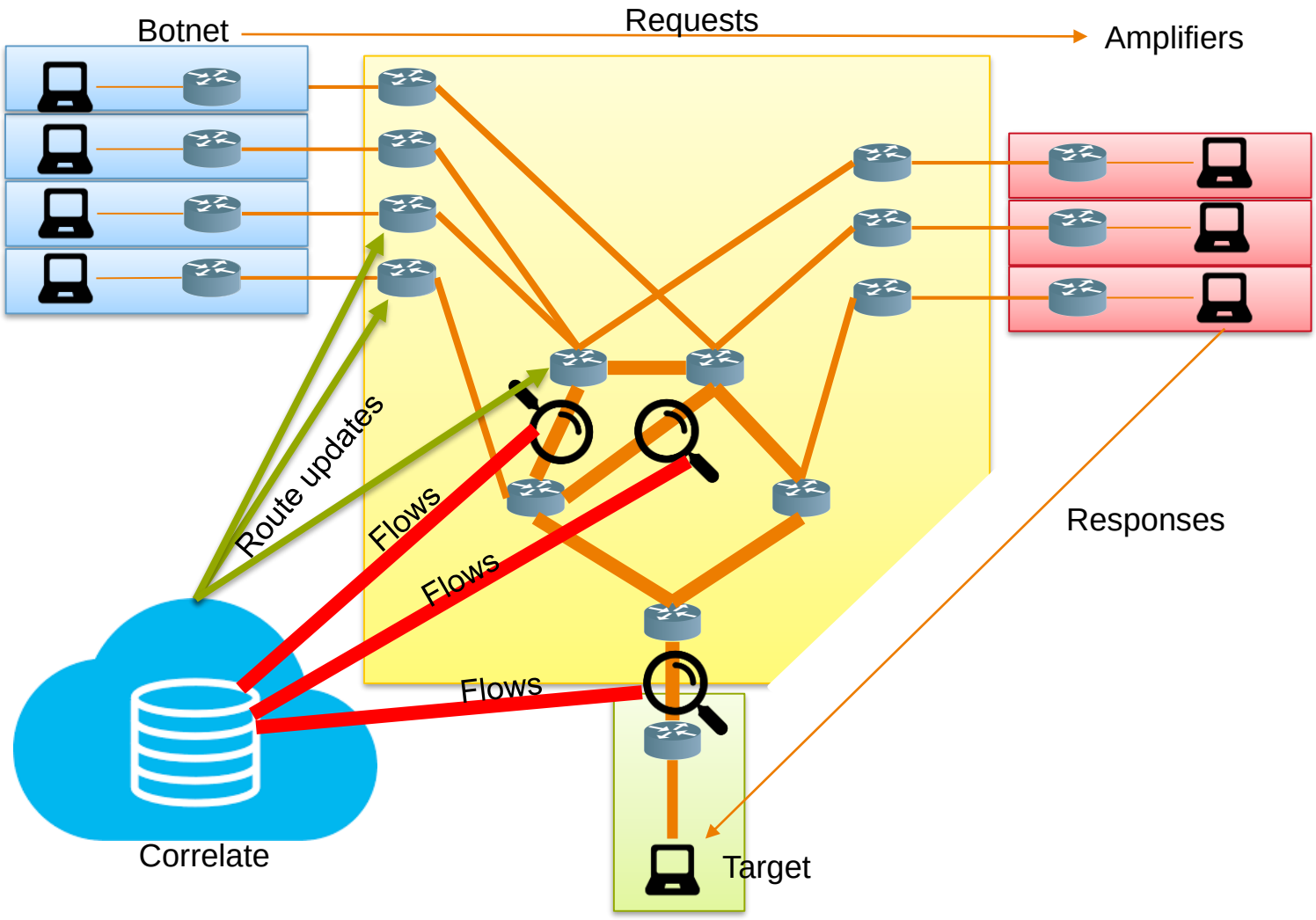
RON'18 IDEAS

TNO innovation for life

DDOS DETECTION IN THE CORE

- DDoS detection in the core is not easy as the volume of the attack does not necessary stand out
  - …as it does near the victim
- Botnet: spoofed srcIP (==target IP), amplifier dstIP
- Possibly we can correlate flows characteristics from the core and edge close to target
  - … or perhaps also close to amplifiers? (Requires SARNET-like information exchange)

- After detection, (automated) action can take place



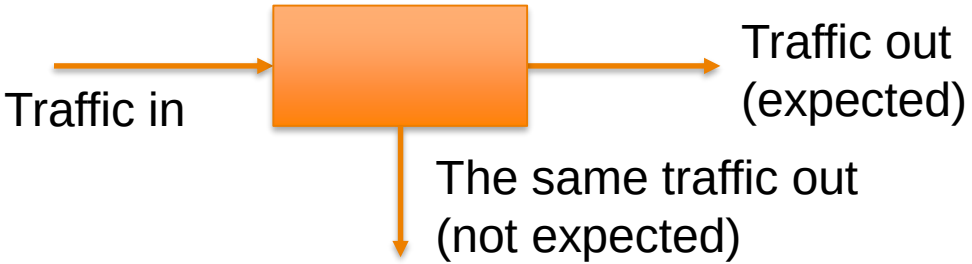
IP + UDP:

- DNS + DNSSEC
- CHARGEN
- MEMCACHED
- NTP
- ….

IP + ICMP

TAPPING/MALICIOUS RELAYS DETECTION

- Belgacom case: traffic from operator's network was tapped
  - https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/
- Can we detect tapping ?
  - If so, at what granularity ?
    - mirror 10G port for months vs. install short-lived flow rule for specific data exfiltration



- Another but somewhat similar threat: malicious relays (e.g., server acting as a router)