An Autonomous Network Management?

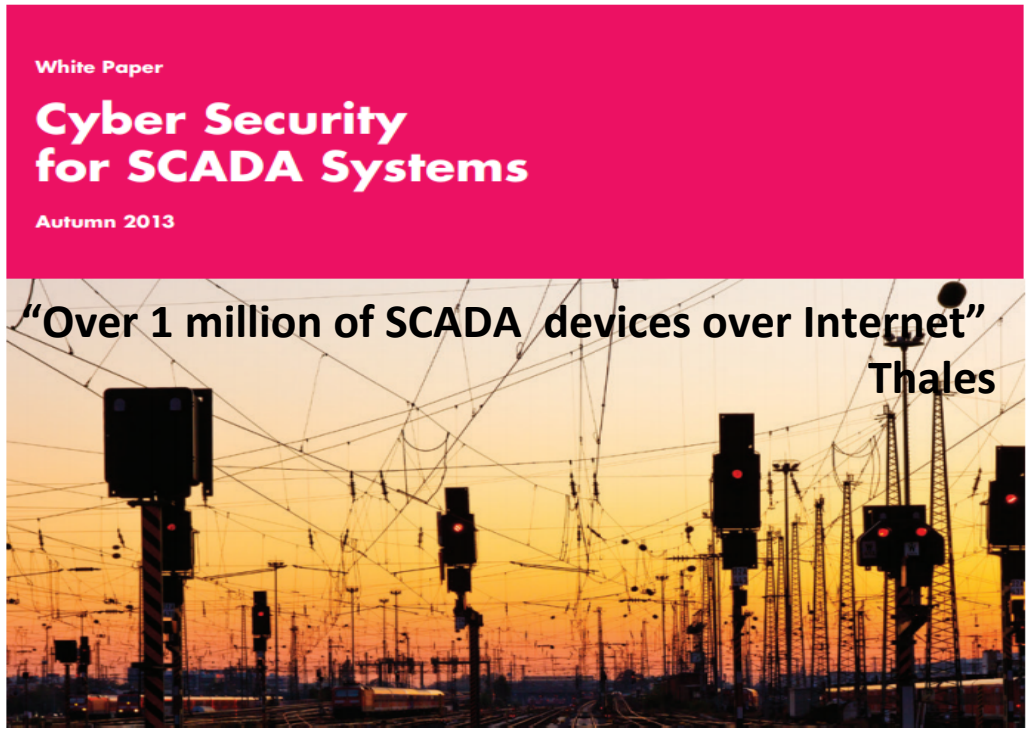
Within the Context of Resilience

Azman Ali, PhD

Telekom Malaysia (Consultant)

Background

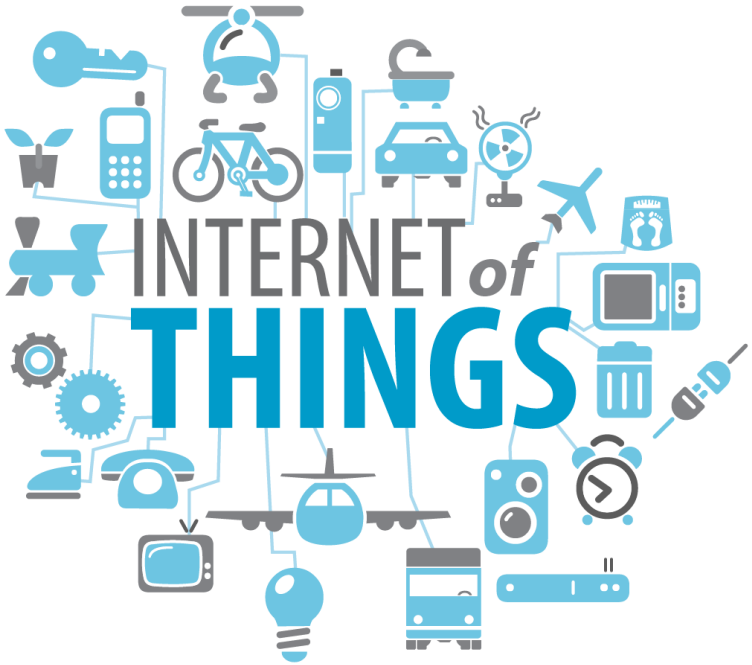
Internet has fast becoming infrastructure for critical services- eCommerce, eGovernment, eSurveillence, DNS, Millions of SCADA/ICS devices, IoTs and other cyber-physical application are currently deployed over Internet



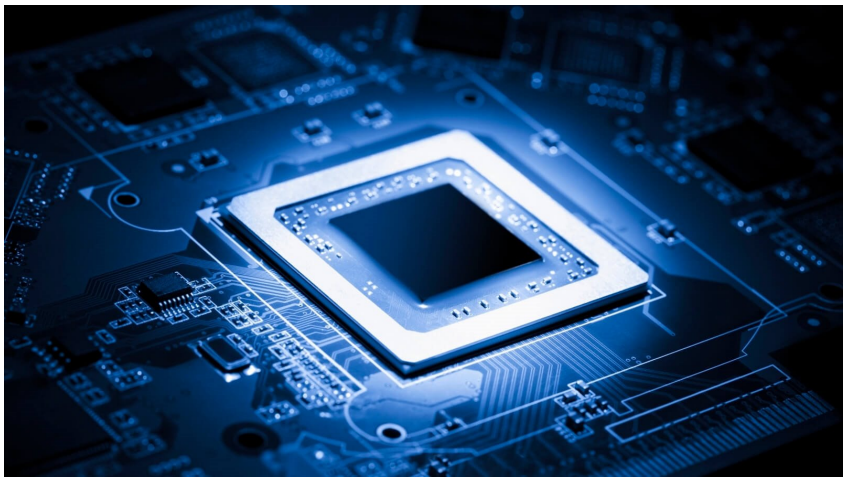
Critical Infrastructure on the Internet attack are still rising (1.2 TBps DDoS on Dyns in 2016, Critical Internet infrastructure brought down by TVs, Camera, smartlights and Toasters)

Background

Internet Traffic (ie Attack) is hard to model : High Volume , High Velocity, Uncertain environment(very Dynamic) . Future (Multilayered) Internet Management needs to address these characteristic.



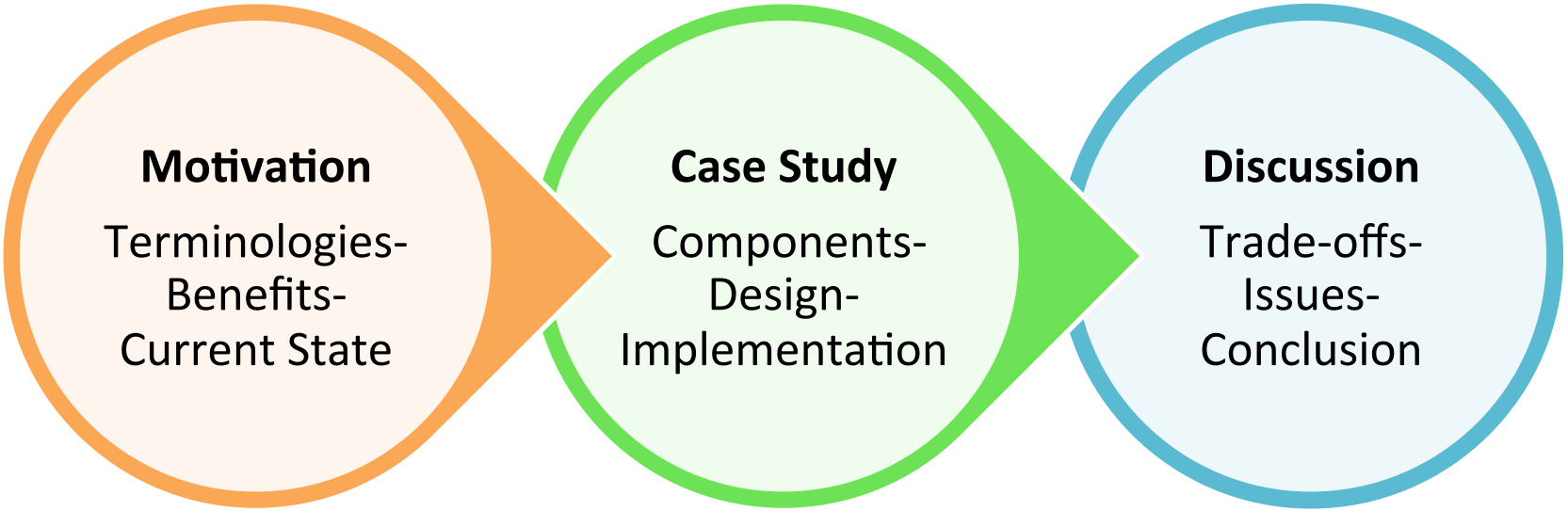
GOOD THING IS THAT SDN, Big Data, Cognitive Computing and **Computational Technology** are evolving,



Autonomous Systems

Introduction

- Autonomous vehicles are already a reality… will the same concept applicable for future Internet Management?



Introduction : The Terminologies

Autonomic and Autonomous refer to the level of Authority.
The idea to to have minimum or no human intervention.

Automatic

Set of fixed/programmed tasks (ie SOP, step by step)

Autonomic

Automation with Intelligent, Self-x (selforganize, selfheal etc), ability to control internal environment/resources)

Autonomous

Self Direction (effect external environment – ie autonomous car, drone)

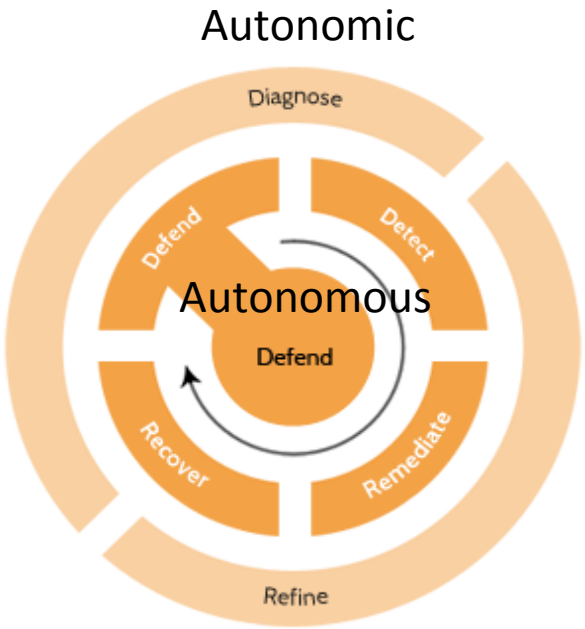
Human Intelligence ← **Intelligence :** Ability to learn, adapt, change, evolve (make decision) → **Machine Intelligence**

Introduction : Resilience

- **Resilience*: Ability to Remain Operation in the face of Challenges***
- **Axiom : Faults are inevitable (Perfect systems are Infeasible)**

- **Example Challenges :** Human Error, Natural Disaster, Attack, Machine Error , Flash Crowd, Sabotage, (some happen with Genuine reasons and not necessarily Malicious)

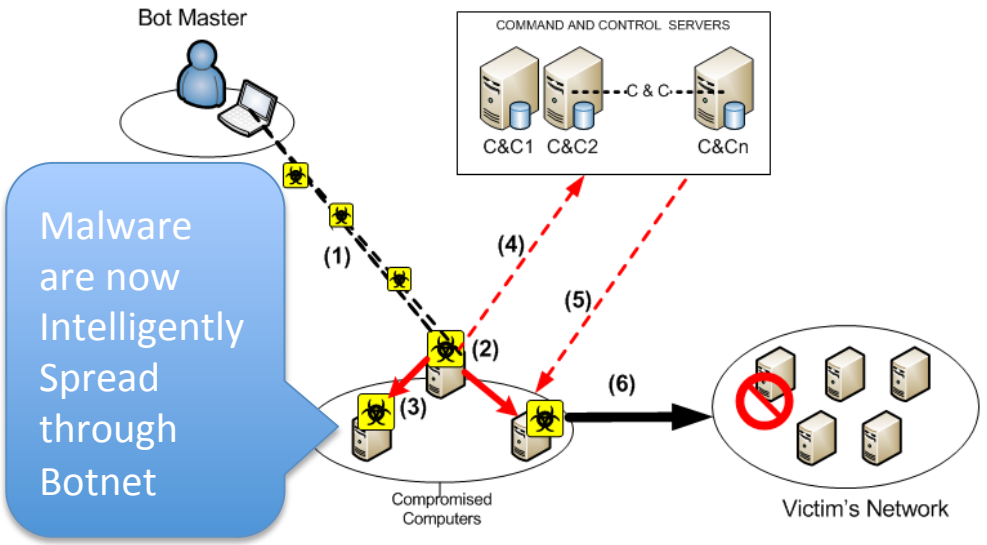
- **Example Strategy :**
  - D^2R^2+DR = Detect Defend Remediate Recover + Diagnose Refine

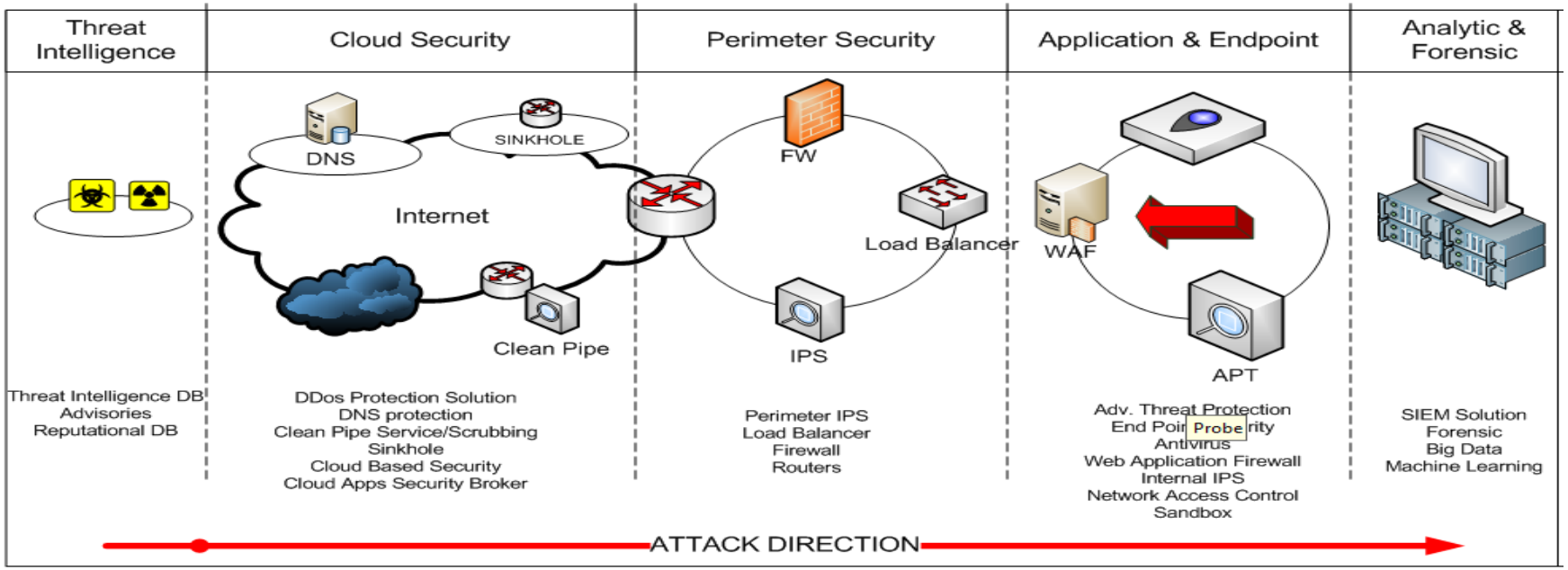


Why: Current State

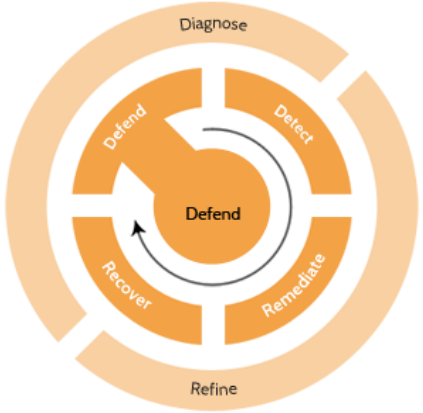
- Current approaches **work in silos** (solutions not designed to fit into multilayer defense strategy)
- Cloud Based services such as **Scrubbing/Clean Pipe** services could be **costly** (ie service cost, bandwidth+ indirect cost)
- **Delay** in Decision making and Action Triggered as most of Security decision are manual
- **Lack of Expertise** within organization to match dynamic nature of challenges
- **Data and Traffic are growing** beyond human capability to analyze or handle (prone to error)

Why? :
Current Challenges
AUTONOMOUS MALWARE
Multilayered .. Need Coordination





Why : The Benefits of Autonomous/autonomic Systems



- **Coordination**- The needs for Orchestration of actions across multiple layers of networks
- **Speed** - Improve Time to Response
  (Real Time decision making and action)
- **Avoid Challenges** that largely due to human factor
- **Retain expertise and experience** within organization
- Human to **Focus of Strategic** rather than technical

How do we do this? : Components of Autonomous systems

AUTONOMOUS

Policy Based Management

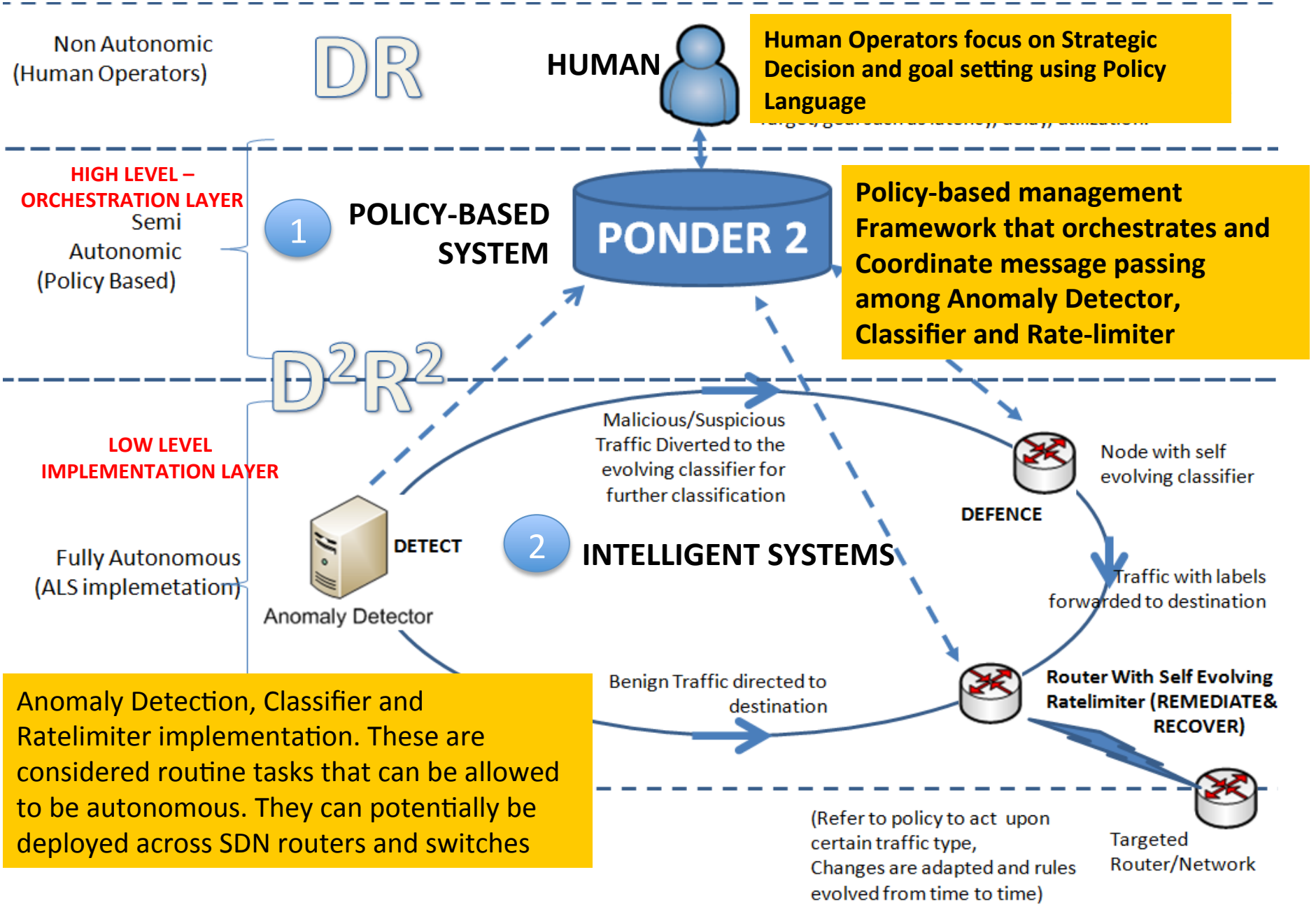
- Take input from user (ie action, parameters)
- Specified by policy Files (ie as strategy lookup)
- Orchestrate Message passing between Network Functions (multilayers/multicomponents)
- Translate/Refine policy to low level implementation (can we use voice recognition?)
- Example : Ponder2 , PonderTalk,

INTELLIGENCE

Intelligent Network Function

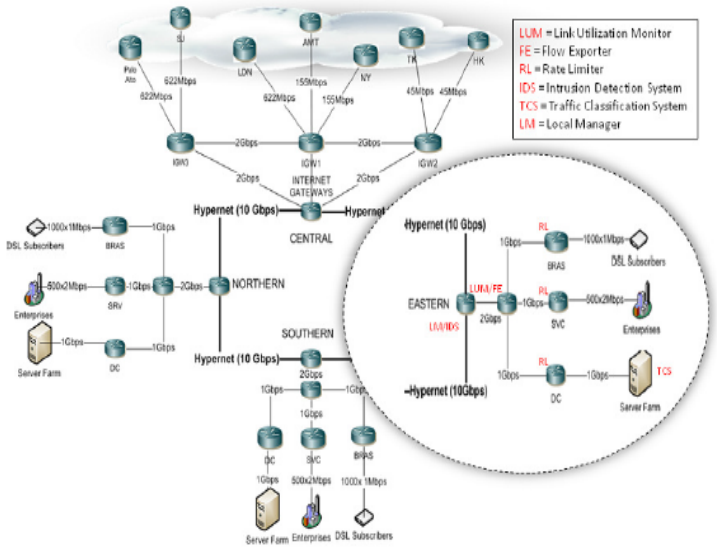
- Decision to be supported by fact
- Perform specific task such as monitor utilization, classify, control
- Triggered through message passing from orchestrator (start, stop, send parameters)
- Performed autonomously until stop directive received

How : Components of Autonomous Systems

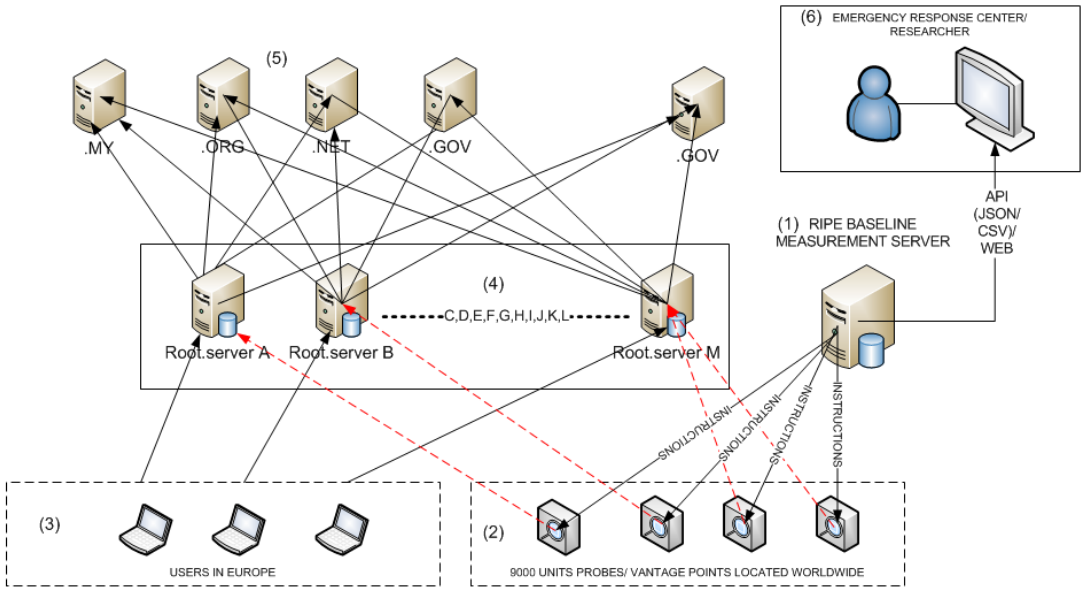


CASE STUDIES : REALIZING AUTONOMOUS SYSTEMS

- The case study was conducted based on 2 scenarios
  - Scenario 1: Simulated DDos using Network Topology of Service Provider.
  - Scenario 2: DDos Detection for DNS root.servers Attack 2015 [1][2]



SCENARIO 1 (Simulated LARGE scale of Attack on Telco using OMNET++ Simulator)



SCENARIO 2 (Anomaly Detection based on RIPE DNS monitoring traffic/queries) [3]

Reference :

[1] http://www.root-servers.org/news/events-of-20160625.txt

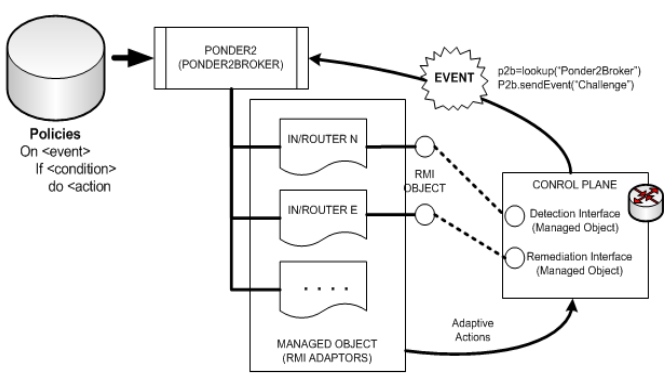
[2] http://thehackernews.com/2015/12/dns-root-servers-ddos-attack.html

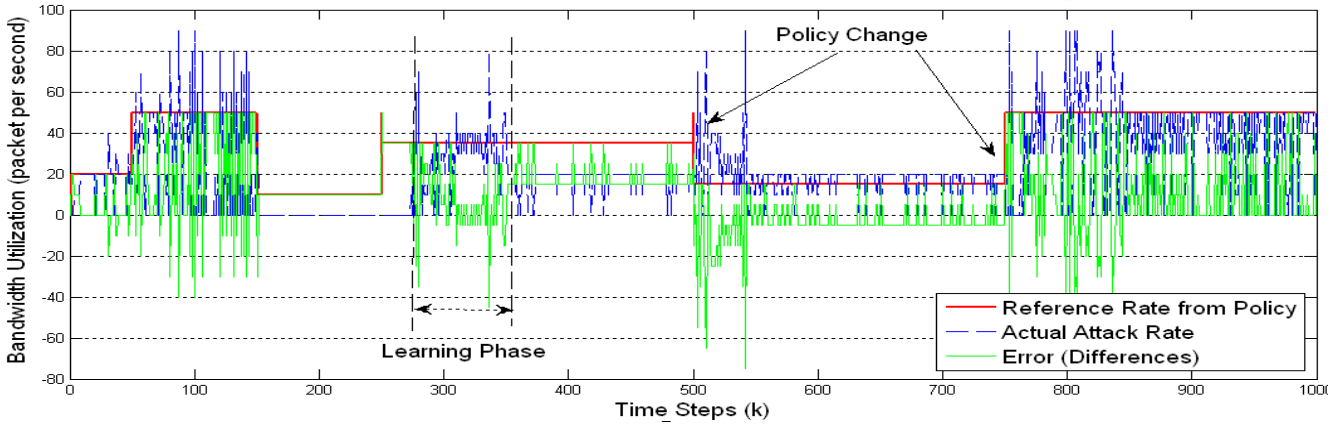
[3] https://www.internetsociety.org/doc/ripe-atlas-probes-and-anchors

CASE STUDIES :Component 1: Policy-Based Mgmt

Ponder 2 : Java based Objects for Policy Management (orchestration) - Ponder2 Framework publicly available

Configure manager for handling high risk alert
on highRisk (link) **if** (LinkMonitorMO getUtilisation() < 50%) **do** RatelimiterMO limit(link, 80%);
on highRisk (link) **if** (LinkMonitorMO getUtilisation() >= 50%) **do** { RatelimiterMO limit(link, 60%); ClassifierMO = **new** KNearestNeighbors(5); ClassifierMO enable(link)); }





Policy autonomously Triggered to change the bandwidth limit (without human intervention)

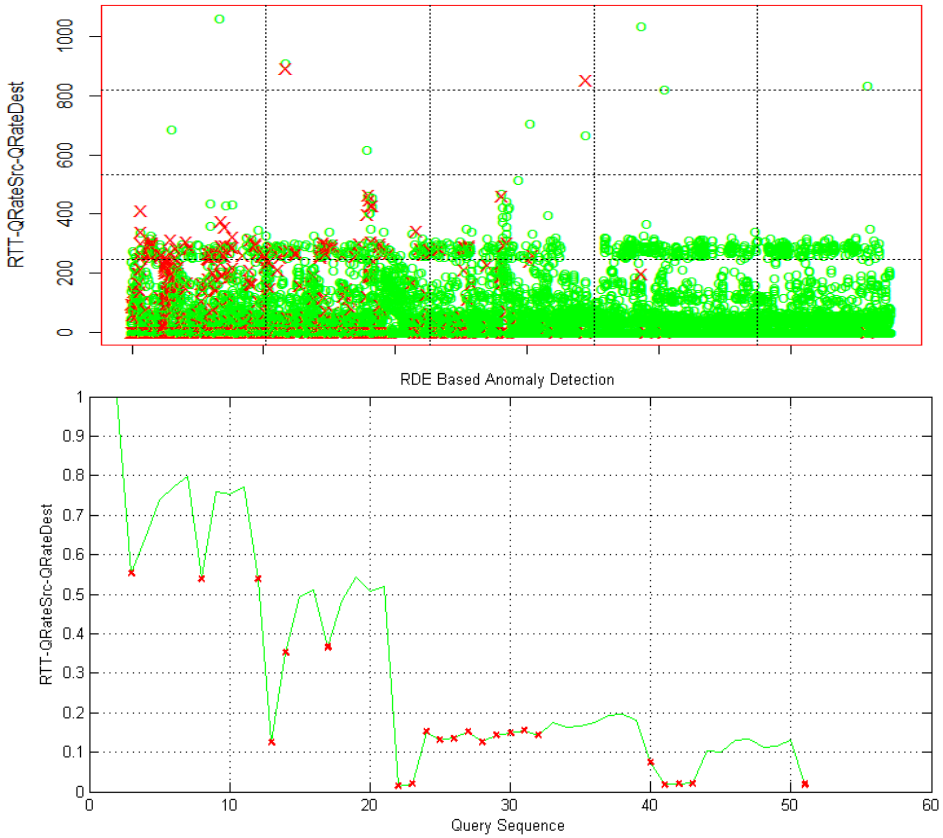
CASE STUDIES – Component 2: Intelligent Systems

Building **Anomaly Detector (using R pogramming)** to detect DNS Attack based on data collected from 9000 RIPE DNS monitoring Probes

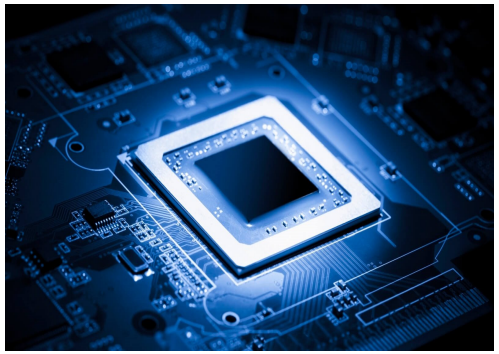
Autonomous Learning Systems Library
Publicly available from : CRAN R Repository

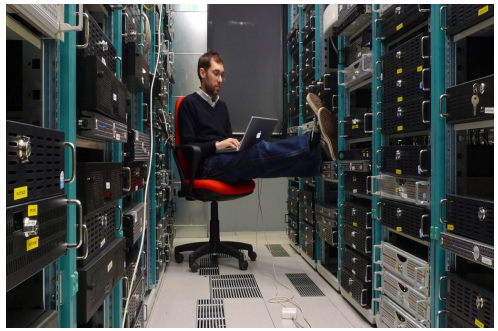
```
for (i in 1:length(avector)){
 if (i == 1){
 a = teda_r(avector[i])
  mean = a$curr_mean
  curvar = a$curr_var
  nexk= a$next_k
     } else {
 a= teda_r(avector[i-1],
       mean,
       curvar,
       nexk)
 mean = a$curr_mean
 curvar = a$curr_var
 nexk= a$next_k
     }
   # r e s u l t [ i ] < -
list(a$curr_eccentricity,a$curr_typicality,
a$curr_norm_eccentricity,a$curr_norm_typic
ality,a$outlier,a$ecc_threshold)
 # summary (a)
```

Attack visualized and and anomaly. Marked in x (in real time). Message can be sent to NMS or passed to orchestrator for automated response (ie trigger other network function such as rate-limiter etc) .



The Drivers and Enablers





- **Technology**
  - Computational Technology (Cheaper and better CPU, memory)
  - Big Data Technology (Machine learning, Deep learning, data visualization, data preprocessing (Extract-Transform-Load) are made easier)
  - Software Defined Network Technology (No more vendor/hardware centricity, allow highly customized use of hardware)
- **Organization**
  - To enable real time decision making and response
  - To Adapt to policy-based management – focus on strategic task rather than routine tasks
  - Business requirement are dynamic due to economic, politic, cultural reason
  - Organizational Mindset and culture (transformation from manual to automation, upskilling, strategic)
- **Individuals**
  - Adequate Skillset and expertise (ie SDN, Phyton, Big Data)
  - Next level for Network/Security Professionals ??

Autonomous Systems Tradeoff and Issues

- Autonomous systems design is subject to **Non-Technical requirement** or policies, sometimes economy, politic or culture related
- **Human In the Loop** should be considered as *emergency switch*
- **Accuracy** may be second priority (after speed and efficiency)

- May **selectively applicable (based on RISK)** to certain type of tasks compared to others (ie routine and low risk tasks can be handled autonomously, but high impact task needs authority intervention)

  - Hence Autonomous systems is recommended at low level implementation level (ie edge analytic+action), but in the context of network-wide deployment it should be autonomic (at the moment)

Other impacts

- More **Intelligence sharing** (multiple providers) which can be from other **context** (ie social media as sensors)
- **New job definitions**, less of low skilled but increased in mid-skilled workers (means more software programming skills?)
- Cultural and **mindset change** (personnel and organizational) – data driven
- Changes are **inevitable**, probably (in the future) needs institutional control or regulations.

Conclusion

- Future Internet Management needs to adapt **Autonomous/Autonomic** and **Intelligent** strategy to address the rise of attack sophistication (& challenges)
- The key components are **Policy-based management** and **Intelligent Systems**
- **Organization and Individuals** are key stakeholders in making Internet Management works
- Better computational, **Big Data** and SDN technology will be technological driver for autonomous systems

Acknowledgement

Reference : wiki.ittc.ku.edu/resilinets/Main_Page

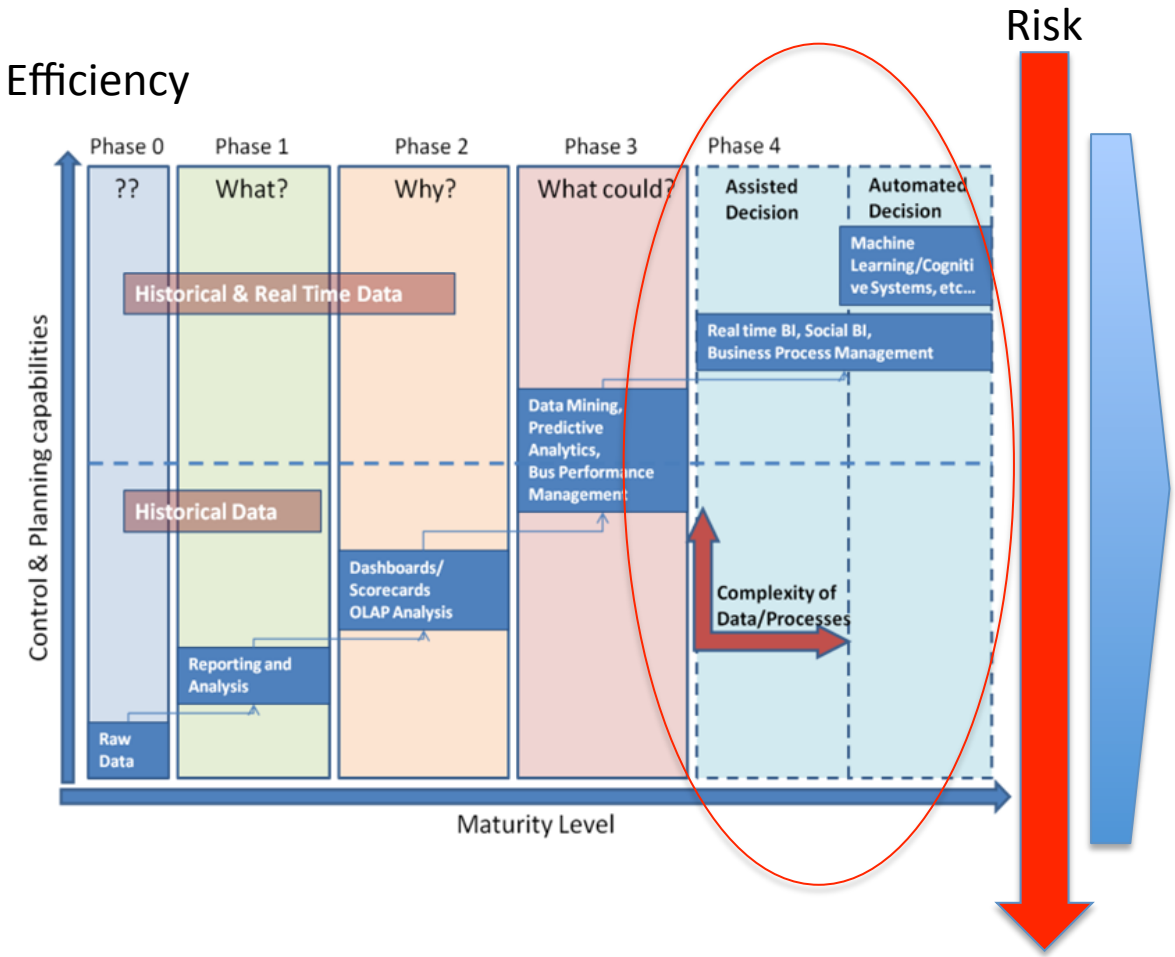
EU Funded Research Framework 7
www.resumenet.eu

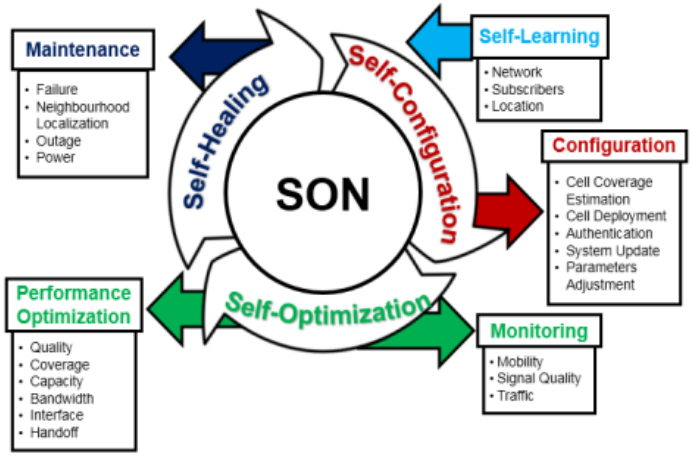
Thank You

Problem Questions

- What is defined as Autonomous Systems?
- What are current state (shortfalls of existing approaches)
- What are the benefits of an autonomous Management of Network?
- What are the Drivers and Enablers
- How does it works/demonstrated?
- Can Network/Internet be autonomously managed? What are the Tradeoff, issues?
- What are the other impacts

Why? : Roadmap to Autonomic Management





https://www3.technologyevaluation.com/research/TEC-report/BI-Maturity-and-Software-Selection-Perspectives.html

https://cognitiveradiosec.wordpress.com/2017/01/28/artificial-intelligence-as-an-enabler-for-cognitive-self-organizing-future-networks/