



Unclouded security



2013.11.08.

Attila Horváth PhD

HUNGARIAN SCIENTIFIC RESEARCH FUND
PD-109740



The Project:

The effects of IT and network vulnerabilities on economy and society

- Growing digital convergence
- Concentration of data, infrastructure and services
- Private/Business/Government
- Critical role of ICT
- Systematic vulnerabilities
- Economic and social effects' assessment for technology based operations/decisions
 - monetary and management approach



Rapid cloud adoption

- IDC: 35% yearly growth rate of cloud services in Western Europa, 15 billion EUR by 2015
- Gartner: 33% of companies already using SaaS for Business Intelligence
- At&T: 37% of companies using cloud to improve business continuity
- Forrester: IaaS penetration:
 - 18% in high tech industries (25% planning);
 - 10% government sector (5% planning)

Customers served

- Google: >500 million android activations/year,
 - US General Services Administration, Essilor, Ispen, BBVA Spain, Capgemini, SNL Financials, Salesforce.com, Essence, The Guardian, LSI Logic, The Telegraph
- Amazon Cloud
 - carry as much as 1% of the all internet consumer traffic in North America
 - a third of all internet users visit an AWS powered site daily
 - Zynga, Animoto, Reddit, MySpace, Netflix, Dropbox, airbnb, Ericssons, European Space Agency, HootSuite, IBM, Mahindra Satyam, Newsweek, UniCredit, Spiegel.Tv, PBS, Yelp, IMDB, Linden Labs, FourSquare, SmugSmug, Alexa, The Guardian, Farmville, Sitepoint, EventBrite.
- Rackspace (>200k customers)
 - Transport of London, Virgin Trains, UK MoD, NHS Direct, Fiverr, Pitchfork, The Register, the Royal Navy, and TweetPhoto
- ...



Cloud Computing is critical

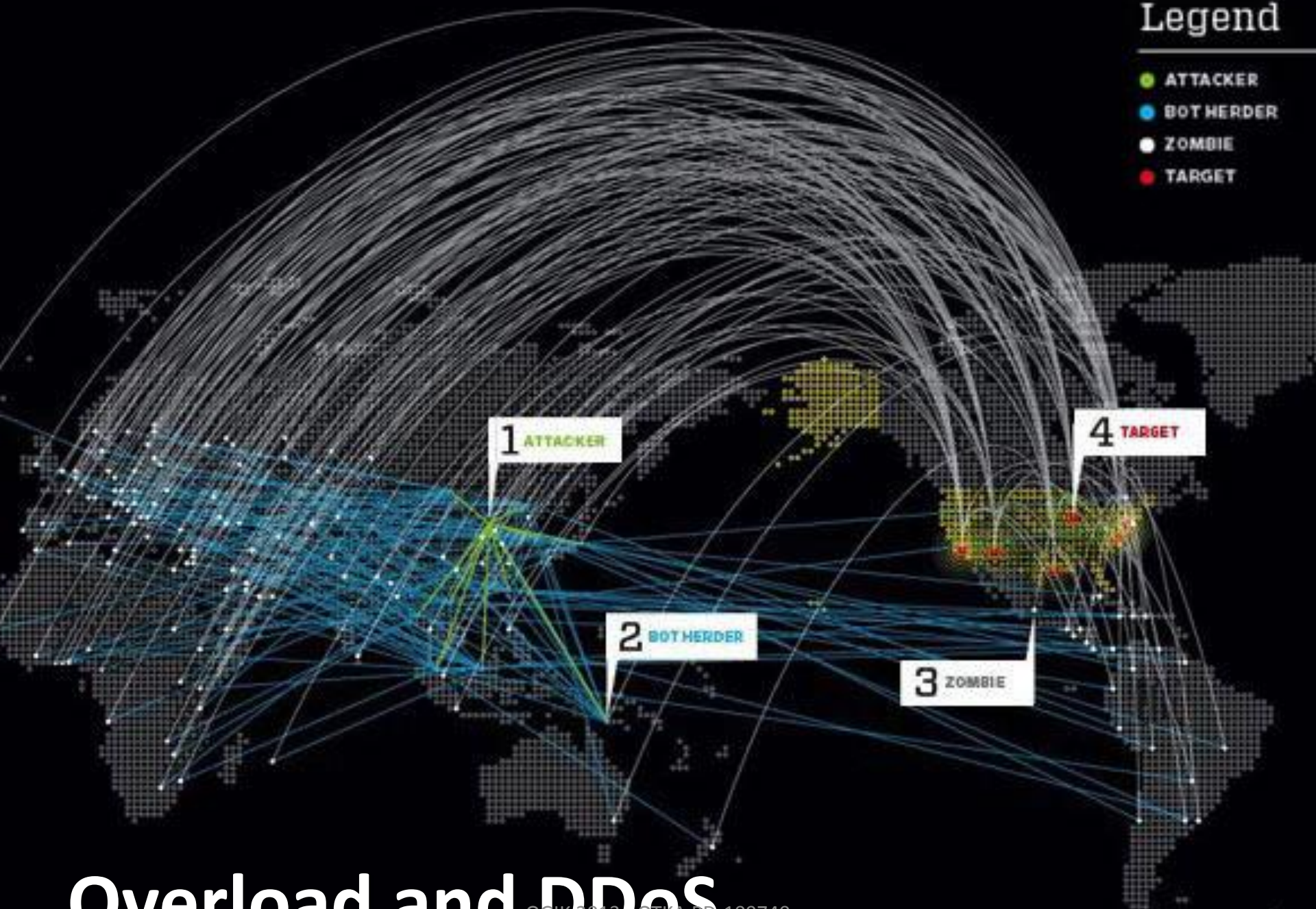
OGIK 2013 - OTKA PD-109740

Protection from natural disasters



Legend

- ATTACKER
- BOT HERDER
- ZOMBIE
- TARGET



Overload and DDoS

Concentrated Cyber attacks

SaaS



PaaS

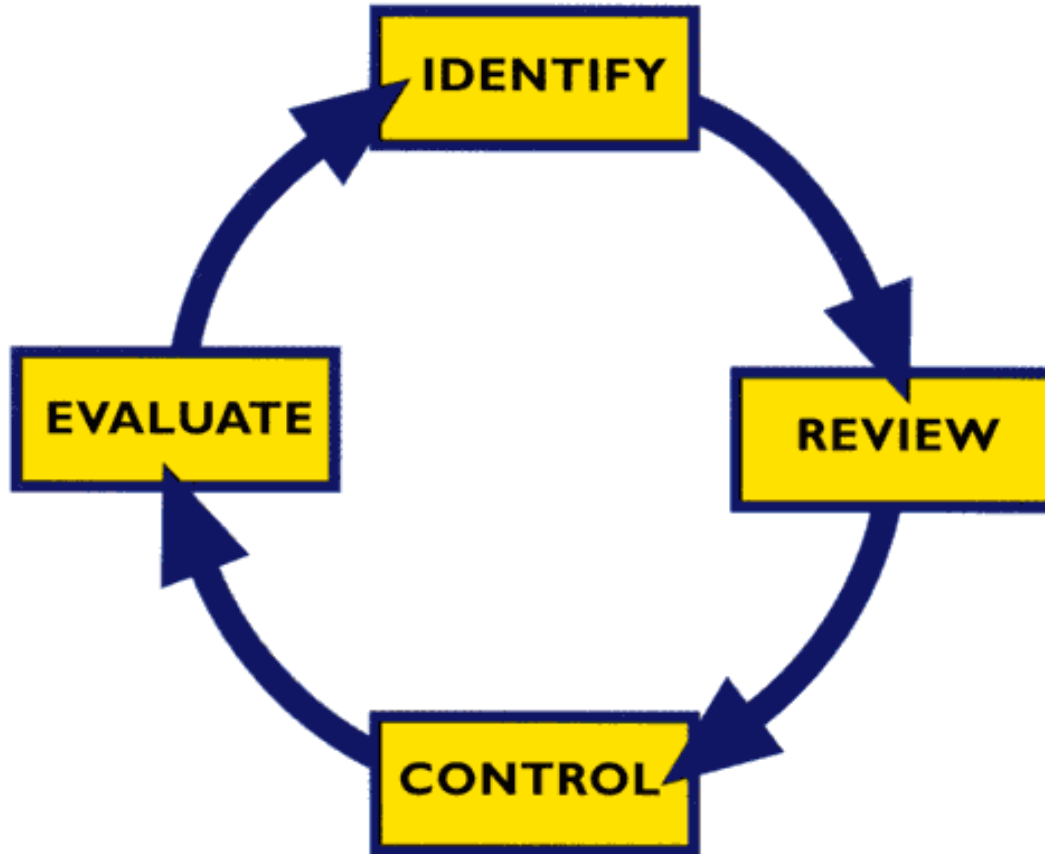


IaaS


Administrative and legal disputes



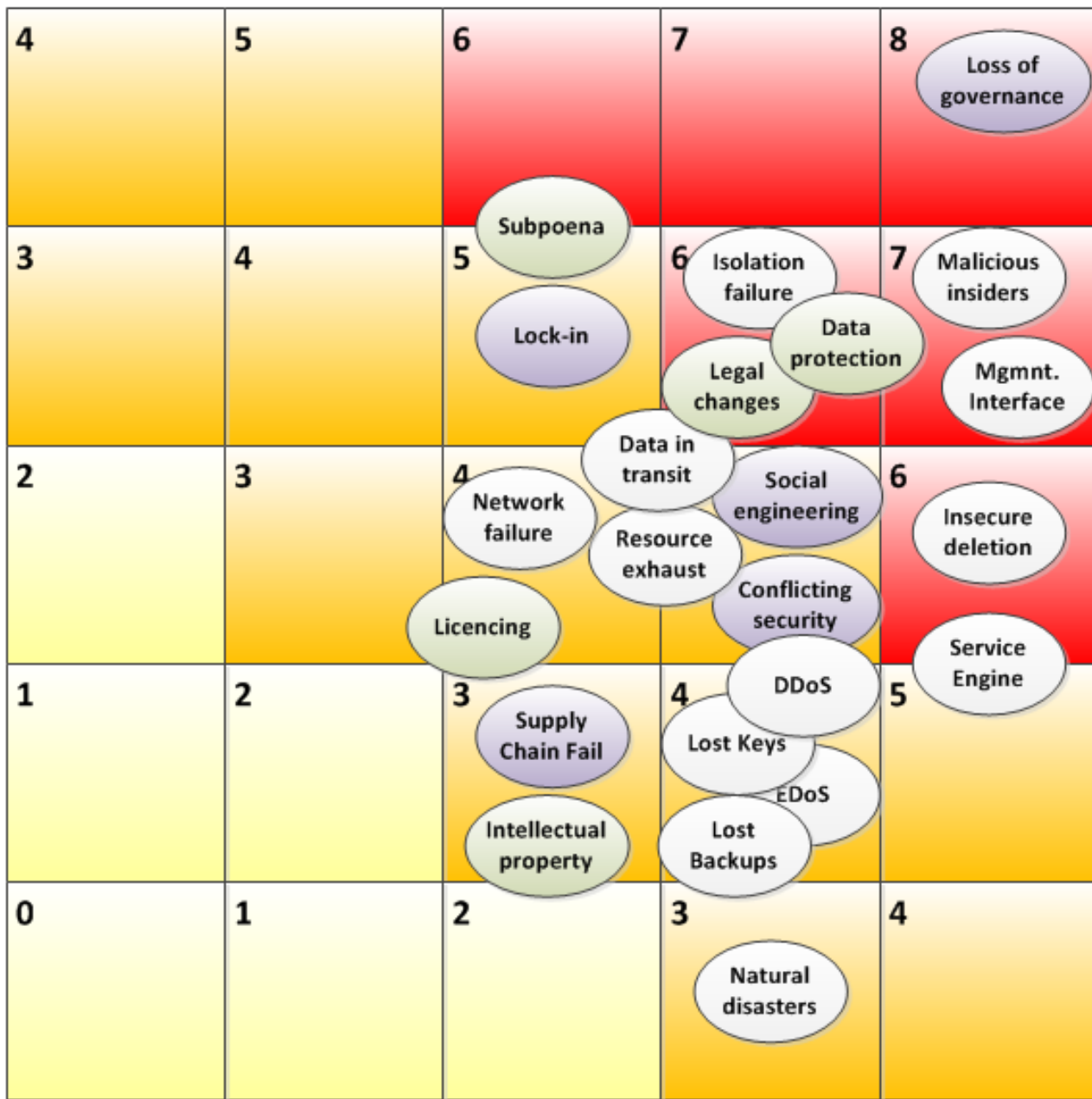
RISK ASSESSMENT



Scope

- Most critical services first
 - IaaS & PaaS
- Dependencies of cloud computing
 - Part of critical infrastructure
 - Same level as Power Supply and Communication
- Transparent thinking – map 
 - Critical operators and critical services
 - Resilience vs. Interdependencies & cascading failures
 - Affecting otherwise unrelated services

PROBABILITY



Organizational risks

Technical risks

Legal risks

IMPACT

SECURITY MEASURES



Best practices

- No real cloud security standards yet
- Best level security is based on best practices
- Knowledge management: support and foster exchange of experiences
- Continuous improvement
- Dangerous if rules are cast in stone
 - Regulator or self-regulation



Logical redundancy

- Physical redundancy is present
 - Different data centers in case of site failure
- Attacks capitalize software vulnerabilities, flaws
 - The same persists on every site
- Logical redundancy is the key
 - Different layers of defense
 - Separate systems with different logical structure
 - Cross-check transactions
 - Intrusion detection



Standardization

- Use of standard APIs is vital
- Avoid issues related to specific provider or platform
- Ease migration
- Move workload to other providers in need
 - Outage
 - System failure
 - Legal or administrative problems
 - Etc.



Monitoring, audits, tests and exercises

- Frequent audit
 - Both internal and external testers
- Certification from third-party auditors is overstressed
 - Security too complex and volatile for and auditor to asses during a „once a year audit”
- Continuous monitoring, audit, test and practice needed



INCIDENT REPORTING



Mandatory reporting

- Understand the impact
- Find the scope
- Reporting thresholds?
- Lack of data
 - Security priorities?
 - Inefficient & ineffective

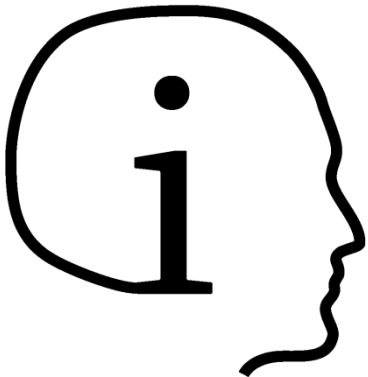


Legal consequences

- Stealthy attacks – difficult to spot
- Hide the traces
- Not reported to management and/or authorities
- Fear from reprisal or legal consequences
- Encourage reporting with incentives



THANK YOU FOR YOUR ATTENTION!



Attila Horváth PhD
horvath.attila@infota.org