Development, Analysis and Evaluation of Cyber Resilience Strategies

Prof. Dr. Axel Lehmann
Prof. Dr. Udo Helmbrecht

Institut für Technische Informatik, Universität der Bundeswehr München, Germany

European Union Agency for Network & Information Security, Greece
Outline

- Expected Trends and Opportunities of the Cyber World
- Cyber Resilience:
  - Requirements, Methods, Challenges
- Objectives & Tasks of the Proposed Project No 12
Setting the scene …

- The world is quickly embracing digital in every part of our life.
- e-banking, e-health, e-commerce, e-education, e-everything are all now totally dependent on an open, safe and secure cyberspace.
- We are witnessing the development and deployment of smart manufacturing, the Internet of Things and computer controlled critical infrastructures.
- Digital is challenging the delivery of old business models, while at the same time providing opportunities for the new world.
- We have to ensure the trust of its citizens and industry to have the necessary confidence to work and live in the digital world.
6 technologies are revolutionizing IT markets ...

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description of technology</th>
<th>Growth trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Big data</td>
<td>Ability to run complex calculations on big amounts of data in a meaningful time frame</td>
<td>Global 33% CAGR 2011-2015</td>
</tr>
<tr>
<td>Sensors and actuators</td>
<td>Introduction of cheap sensors and actuators to collect huge amounts of data</td>
<td>Potential $4-11 economic impact estimated in 2025</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>Hosting of software on centralized servers with high-speed access through the Internet</td>
<td>Global 27% CAGR in public cloud services revenues</td>
</tr>
<tr>
<td>Mobile technology</td>
<td>Massive increase of mobile computing power, storage, and bandwidth</td>
<td>Global 27% CAGR in mobile-to-mobile communications revenues</td>
</tr>
<tr>
<td>Natural user interfaces</td>
<td>Creation of new kinds of interfaces that allow for more intuitive handling of IT systems</td>
<td>30% reduction in page visits per click</td>
</tr>
<tr>
<td>Computation, storage, and networks</td>
<td>Possibility to store large amounts of data and transfer the data with high bandwidth between computers</td>
<td>Global 15% CAGR in enterprise storage market</td>
</tr>
</tbody>
</table>

SOURCE: Gartner, MGI, Team analysis, CAGR = compound annual growth rate

Lehmann/Helmbrecht ICT Resilience Erice 2016
# 5G mobile communication

## WHAT IS 5G?  CONTRIBUTION OF EU RESEARCH

<table>
<thead>
<tr>
<th>What 5G will bring to you?</th>
<th>What’s new with 5G?</th>
<th>EU projects</th>
<th>5G applications</th>
<th>Why not today?</th>
</tr>
</thead>
<tbody>
<tr>
<td>amazing volume</td>
<td>spectrum extension; millimetre waves; cell densification; increase spectrum efficiency; advanced antennas; 5G beamforming techniques; new electronic components; backhaul optimization; D2D, moving networks (vehicle based cells)</td>
<td>[Image]</td>
<td>hologram TV, immersive presence, augmented reality, ultra large volume transfers</td>
<td>spectrum valuation; limited spectrum aggregation; current hardware not able to function at high frequencies; expensive deployment &amp; maintenance of small cells</td>
</tr>
<tr>
<td>amazingly fast</td>
<td>combination of 4G, 5G, Wi-Fi, &amp; new radio access to create an integrated &amp; dynamic radio access network, connectivity management mechanisms</td>
<td>[Image]</td>
<td>staying connected everywhere including high-speed trains, planes, crowds</td>
<td>seamless handover (e.g. cellular to Wi-Fi) not supported</td>
</tr>
<tr>
<td>always best connected</td>
<td>ultra-low latency; software-defined networks; decoupling functional architecture from the underlying physical infrastructure; network intelligence closer to users; MEC (mobile edge computing); D2D</td>
<td>[Image]</td>
<td>tactile internet; reactive interfaces; electricity grid control; vehicle to vehicle; robot control; connected cars, remote surgery</td>
<td>4G latency &gt; 10ms</td>
</tr>
<tr>
<td>no perceived delay</td>
<td>millimetre waves for front-haul &amp; backhaul; new operation mechanisms for dense networks; pooling of base station processing; on-demand consumption massive machine communications; power amplifiers; DSP (digital signal processing) - enabled optical transceivers; harvesting ambient energy; optimization of sleep mode switching</td>
<td>[Image]</td>
<td>internet of things, smart cities, connected cars, e-health</td>
<td>current OFDM waveform limitations; interference prevents scaling up; 4G chokes cost; energy consumption</td>
</tr>
<tr>
<td>massive amount of</td>
<td>new waveform; cell densification; much less signalling traffic &amp; no synchronisation; RAN architecture</td>
<td>[Image]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>connected things &amp; people</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>energy efficiency</td>
<td>millimetre waves for front-haul &amp; backhaul; new operation mechanisms for dense networks; pooling of base station processing; on-demand consumption massive machine communications; power amplifiers; DSP (digital signal processing) - enabled optical transceivers; harvesting ambient energy; optimization of sleep mode switching</td>
<td>[Image]</td>
<td>80% energy saving; deployment in developing countries</td>
<td>Base stations idle time not optimised; unused functions activated; air interface/hardware not energy optimized</td>
</tr>
<tr>
<td>flexible programmable</td>
<td>software-defined networks; network function virtualisation; decoupling functional architecture from the underlying physical infrastructure; APIs</td>
<td>[Image]</td>
<td>new business models for innovative SMEs providing network functions; emergence of super MVNOs; pan European operators, faster innovation in network services</td>
<td>many various network management software; not interoperable; bundling of network functions in hardware boxes</td>
</tr>
<tr>
<td>networks</td>
<td>physical channel authentication; virtualised authentication</td>
<td>[Image]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>secure networks</td>
<td></td>
<td>[Image]</td>
<td>networks for police &amp; security professionals; privacy</td>
<td>Security as add-on not by design; fragmented approach</td>
</tr>
</tbody>
</table>
Opportunity 1: Smart Grids

From: http://cleantechnica.com/2014/02/19/global-smart-grid-investment-grows-china-leads-us-falls-behind

Lehmann/Helmbrecht
ICT Resilience
Erice 2016
Opportunity 2: Smart Homes

Image: http://www.refitsmarthomes.org/index.php/about/

Lehmann/Helmbrecht ICT Resilience Erice 2016
Opportunity 3: eHealth

Challenges

Complex networks and services
Low quality software & hardware
Asymmetric threats allowing remote attacks
Increasing organised cybercrime and industrial espionage
Lack of international agreements and regimes
Why Cyber Security is a Planetary Emergency

Tesla driver dies in first fatal crash while using Autopilot mode

The autopilot sensors on the Model S failed to distinguish a white tractor-trailer crossing the highway against a bright sky.

> Learn from:

* Why the culture of safety is a critical concern for the future expansion of nuclear power
Dr. Robert Budnitz – Lawrence Berkeley National Laboratory, Berkeley, CA, USA
Outline

- Expected Trends and Opportunities of the Cyber World
- Cyber Resilience:
  
  Requirements, Methods, Challenges
- Objectives & Tasks of the Proposed Project No 12
Definition: Resilience of a System

“... the ability of an organization or a system to continue to carry out its mission during a disruptive event and then return to normal operations once the stress of the disruption is relieved”

(US Dep. of Homeland Security)
Resilience Analysis ..... 

.... requires to consider 4 stages of event management to maintain system resilience:

- **Plan/prepare** (w.r.t. malfunction, failures, attack, etc.)
- **Absorb** (isolating disruption)
- **Recover** (return to pre-event functionality, performance)
- **Adapt** (implement lessons learned)

*(National Academy of Sciences)*
Resilience of a System in Cyber Space …

- … has to consider ...

- > ubiquitous, pervasive, mostly invisible computing

- > interconnectivity between (sub-)systems
  -> “System-of-Systems”

- > global connectivity through internet
  -> “hyperconnectivity” (World Economic Forum)
Resilience

Threats

Means

Metrics (ref)

Domain

ThreatAgent

confronts

isEnabledBy

isExpressedBy

isNeededBy

isThreatenedBy

Lehmann/ Helmbrecht

ICT Resilience

Erice 2016
For Resilience of Critical Infrastructures …

- ….. 5 strategic layers have to be considered:
  - Global layer
  - Enterprise / Private layer
  - Information layer
  - Technology layer
  - Physical layer

- Simulation-based analyses of propagation of disruptive events through the layered system architecture
  (dependency graphs; SATURN: Self-Organizing Adaptive Technology Underlaying Resilient Networks)

( Creese, Goldsmith, Adetoye, IEEE, 2011)
Important Factors of ICT- / Cyber-Resilience Engineering

- **Minimizing risks** caused by faults, errors, failures, misuse, attacks, accidents or disasters in ICT-systems:

  \[ ICT{-}\text{Risk} = \text{Threats} \times \text{Vulnerabilities} \times \text{Assets} \]

- **IT- / Cyber Resilience Engineering requires:**
  - Identification of key IT assets
  - Controls to protect those assets from harm
  - Ability of those systems to operate under stress and recover from disruptive events
  - Processes for ... protection and sustainment activities
  - Development of appropriate metrics and measures
Expected Major Trends of ICTs ....

... technological innovations, e.g.:

- Low-energy-consuming Micro-... to ...High-Performance-Computers (Exabyte)
- “More Moore” & “More than Moore” on a chip ->
  -> Cost-effective sensors /actors
  -> Cyber physical systems
Expected Major Trends of ICTs ....

... organization / computing principles, e.g.:

- Organic computing: self-x-properties,
  
  \((x = \text{adapting, organizing, repair})\)

- Neural computing (artificial neural nets)

- Artificial Intelligence applications
Expected Major Trends of ICTs ….

…. lead to major chances & risks:

- Increasing interconnectivity between components & systems
- Evolutionary “System of Systems” development
  - Increasing size of a system’s state space
  - Emergent system behaviour !!!

- Key challenge w.r.t. cyber resilience:
  - “Mastering” System-State-Space-Complexity of ICT-systems /-applications !!!??
Major Problem of Ubiquitous Computing & Communication ....

- ... is „System State Space Explosion“:

  - Simple functional analysis requires:
    - reachability analysis for each state in state space
    - feasible for state space size $\leq 10^{100}$ !!

  - Numerical Analyses (of non-functional parameters, e.g. performance / reliability)
    - for state space: $\leq 10^8$ (approx. < 1/2 day on a PC)
    - $\leq 10^9$ (still computable on a PC)
    - $\leq 10^{10}$ (on a PC Cluster)

⇒ Full state space exploration is practically impossible:
⇒ result in emergent system behaviour !!
Conclusions

✿ **Summary**

- Key Challenge: How can we master the (system state space) complexity of ubiquitous ICT-systems!? 

✿ **Conclusion**

- Need to better understand / analyse emergent systems behaviour (by mathem. modelling & simulation)
- Intelligent control for protection and self-adaptation
- Policies (principles)
- Standards & Guidelines
- Tests for validation & certification
Development, Analysis and Evaluation of Cyber Resilience Strategies

Outline

- Expected Trends and Opportunities of the Cyber World
- Cyber Resilience:
  Requirements, Methods, Challenges
- Objectives & Tasks of the Proposed Project No 12
Proposed Project:

- Efficient concepts and algorithms for system state space exploration (e.g. by model checking)
- Identification of major sources of ICT vulnerabilities and risks
- Development of efficient mathematical and logical modeling methods (e.g. Markovian models, reasoning methods)
- Simulation experiments (e.g. data farming) for risk and vulnerability analysis
- Analyses and evaluation of resilience strategies
Thank you very much for your interest and attention!