At the Dawn of The Information Society:
About the Roles of Risk and Security in the Information Society

Dr. Klaus Brunnstein
Professor for Applications of Informatics
Faculty for Informatics, University of Hamburg

3rd International Conference on IT-Incident Management & IT-Forensics (IMF-2007)
Stuttgart September 11-12, 2007

Content:

1. **Evolution of Digital Technologies (DTs) in the „Information/Knowledge Society (IS/KS)“**

2. **Granular Structure of Digital Technologies (DTs)**

3. **Risk Analysis of Digital Technologies**

4. **Approaches to Safe and Secure DTs**

1.0 Roles of DTs in the „IS/KS“:

.1 Lessons learned from „Industrial Society“

- Analogies between Industrial and Information Economy
- Stage 2: Technical limits of electromagnetic solutions
- Beyond Stage 2: changing technologies and paradigms

.2 „Digital Relations“ replace „Human Relations“

- Examples of Digital Relations

1.1a Roles of DTs in the „IS/KS":

Physical Goods | **Virtual Goods**

Sector A **Sector B** **Sector C** **Sector D** **Sector E**

Ressources Products Services Ressources Products

Pre-Industrial Economy

Agriculture +++ Transport ++ KnowHow+ Books+
Manufacture ++ Organisation + Media+

Industrial Economy

Industry +++ **Transport++** **KnowHow ++** **IPR+**
Agriculture ++ **Managemnt++** **PublicInfo+** **Media+**

I-Economy
K-Economy
I-Society
K-Society

Industry ++ **I-Production/I-Commerce+++**

I-Access+++ **I-Bases+++**

Agriculture + Transport ++ **VirtualTransport+++**

<=================== Virtual Organisation

1.1b Analogies: Industrial vs. Information Economy

- **Machines (Engines)**: driven by steam, electricity, oil, gas; development in several phases
- Inherent Insecurity: exploding steam engines killing workers → manufacturers start improving machines
- **Growingly complex "systems"**, growingly difficult to control industrial artefacts (e.g. Titanic)
- **Inadequate Safety: Cars/„**UnReliable at any Speed!" (R. Nader) → Development of Customer Legislation
- **Risk of Controlling Complex Physical Engines**
- **Quality of Products/Methods** developped slowly
- **Production**: on micro-scale (linked factories/offices)
- **Impact on Legal System**: customer protection

1.1c Analogies: Industrial vs. Information Economy

- **“Information Engines”:**

  Single Systems: Mainframes ... PCs ... Microprocessors..

  Networked "Systems: Hardware/Software/Agents/Orgware

- **Information as Product and Production Method**:
  - "Net-Work": TeleWork, TeleBanking, TeleLearning, ...
  - Stored Information, Distributed Processing (Agents!)

- **Complexity** grows beyond control of experts

  Example MS-Windows: “UnReliable at any Speed!”

- **Risk**: How to **Control Complex Virtual Engines?**
  - Fatalistic user action after system failure: Ctrl+Alt+Del
  - Import of potentially harmful active content
  - Connection to search engines without limitation of import (Cookies, Profiles) or export (e.g. registrar content)

1.1d Stages (1- 4) of the „Industrial Economy“

- **Schumpeter, Kondratieff:**
  Model for industrial development (international competition),
  for last (2) phases of Industrial Society (Supply-side of markets)

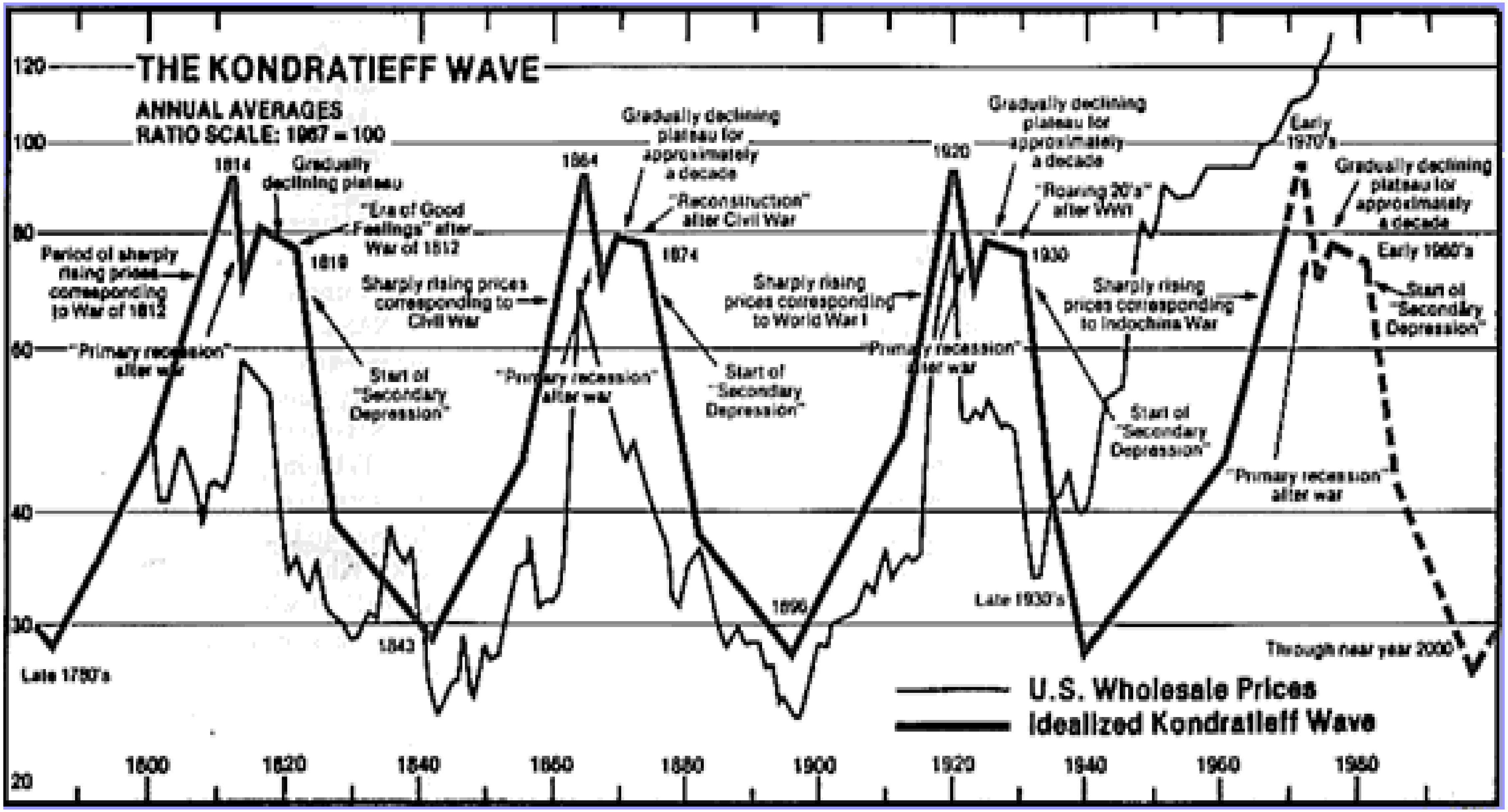
- **Nefiodov: Model applied** to **Generic Technology and extended** backward **to preceeding phases** (1-2):
  - **Phase 1** (1760+): Vapor driven stationary engine (external combustion)
  - **Phase 2** (1810+): Vapor driven mobile engine

→ Paradigmatic change in lead technology!

  - **Phase 3** (1860+): Oil-driven engines (internal combustion)
  - **Phase 4** (1910+) Electricity-driven engines, networks

=Precondition for computing/networking!

1.1e Kondratieff: Cycles of Industrial Economy:



1814 1864 1920 1970

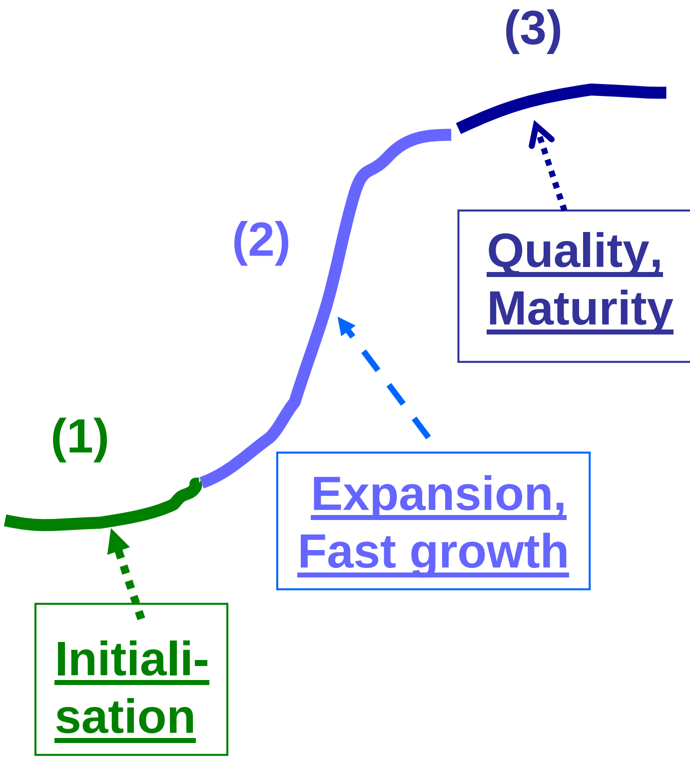
1.1f Special Aspect: Conditions of Lead Technologies

Paradigm of Kondratieff cycles:

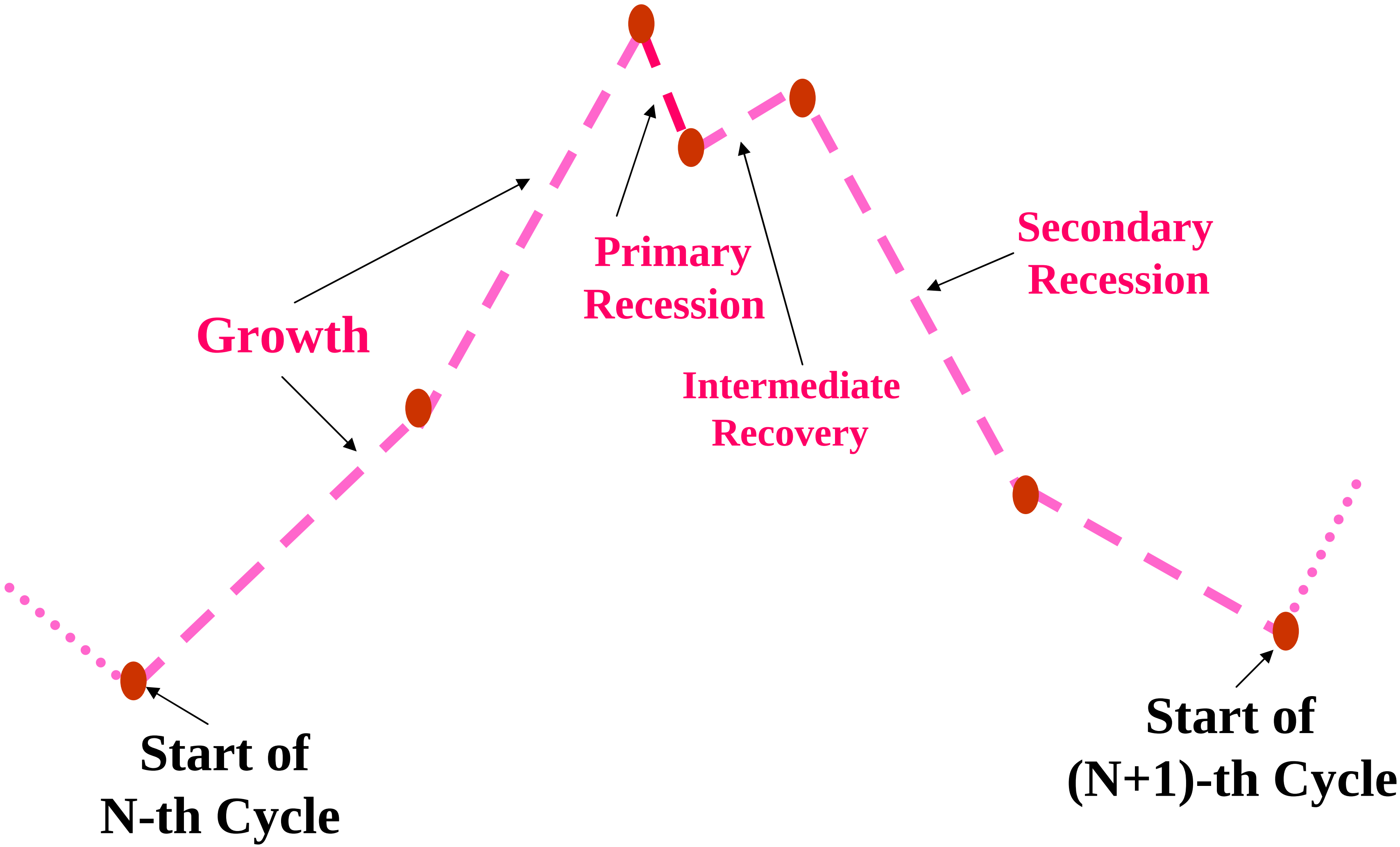
A „Lead (=Key) Technology“ has the power to induce a development cycle (about 40-50 years), with the following phases:

(0) From appearance of technology,
(1) few applications of technology demonstrate its power in the 1st phase.
(2) In 2nd phase, technology is applied to as many applications as possible.
(3) With reduction in new applications, more weight is put on quality assurance: technology becomes „mature“.

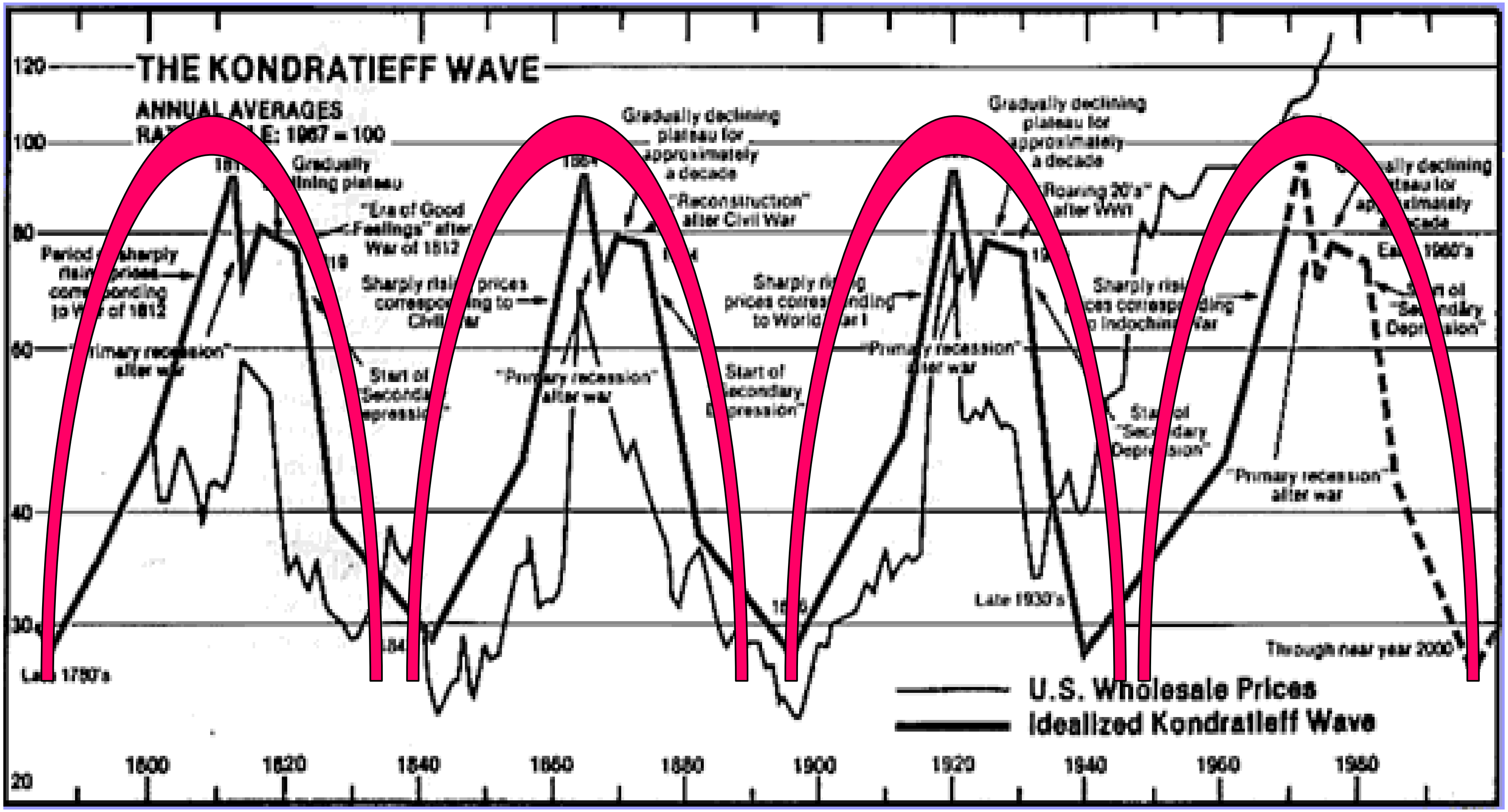
As this technology is „exhausted“ after phase 3, another lead technology will have to start shortly before the end of phase 3.



1.1 g Fine Structure of a Kondratieff Cykle:



1.1h Kondratieff: LeadCycles of Industrial Economy:



1814 1864 1920 1970

1.1h1 Stages (1-2) of the „Information Economy“

- **Assumption**: **„History repeats, though with adaptation“**
- **Adaptation of Schumpeter/Kondratieff Model**

Lead Technology: Use of electromagnetic phenomena for Storage, Processing, Transmission:

– **Phase 1** (1940+): **Stationary Systems**
  - **From Mainframes to Midis to PCs To Integrated Circuits (ICs) to Embedded/RF ICs.**
  - **Stationary systems:, local code/control;**
  - **Development driven by Computer-companies**

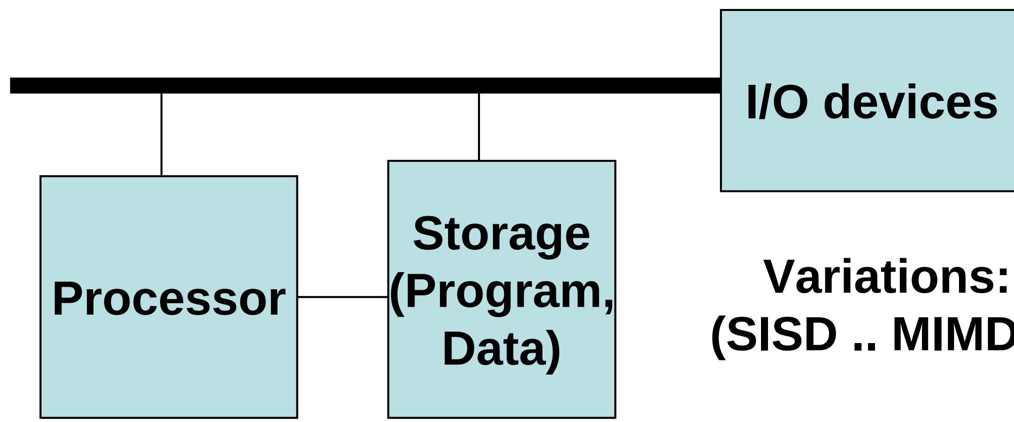
- **Phase 2 (1980+): Network and Mobile Systems**:
- **LAN ... WAN, mobile code/agents, data searching&mining, value-added services**
  - **Development driven by Network companies**

1.1j Phase 2 of The „Information Economy“

Evolution of System view of „Net-Work“:

From von Neumann´s EDVAC .....:

EDVAC: Electromagnetic
Discrete
Variable
Automatic
Computer

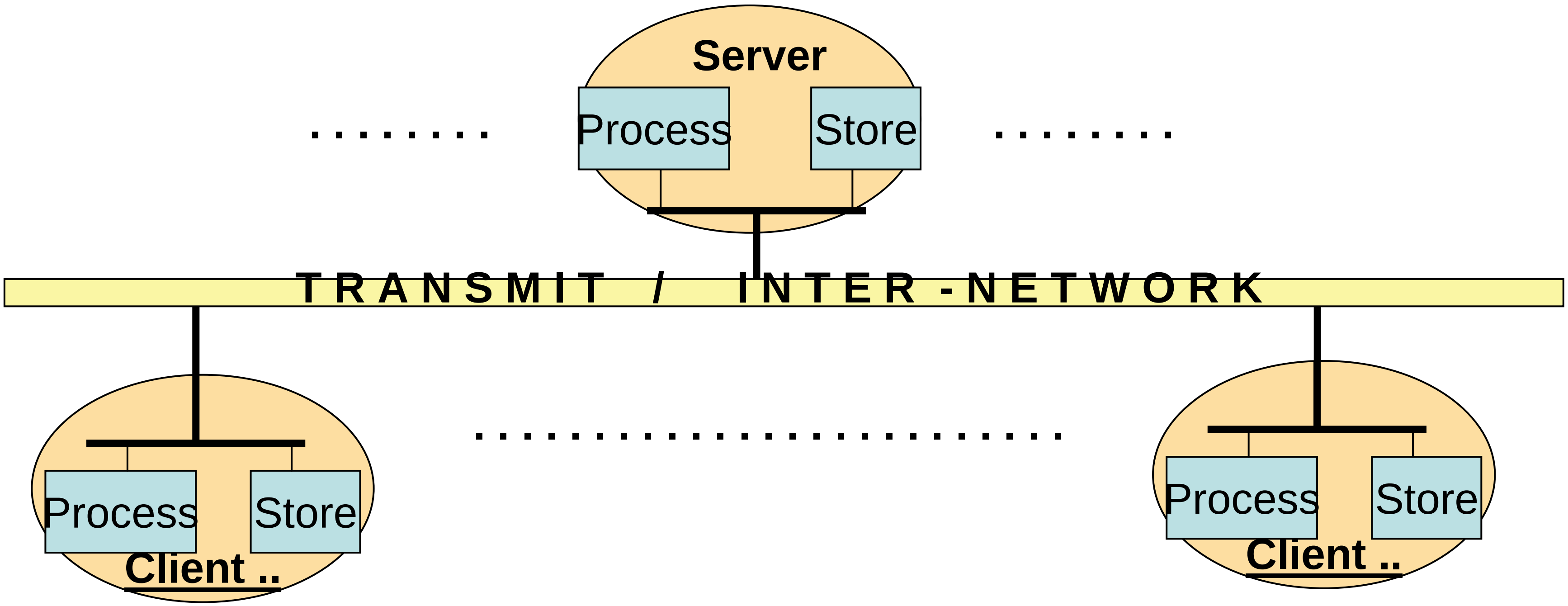


Variations:
(SISD .. MIMD)

1.1j1 Phase 2 of The „Information Economy“

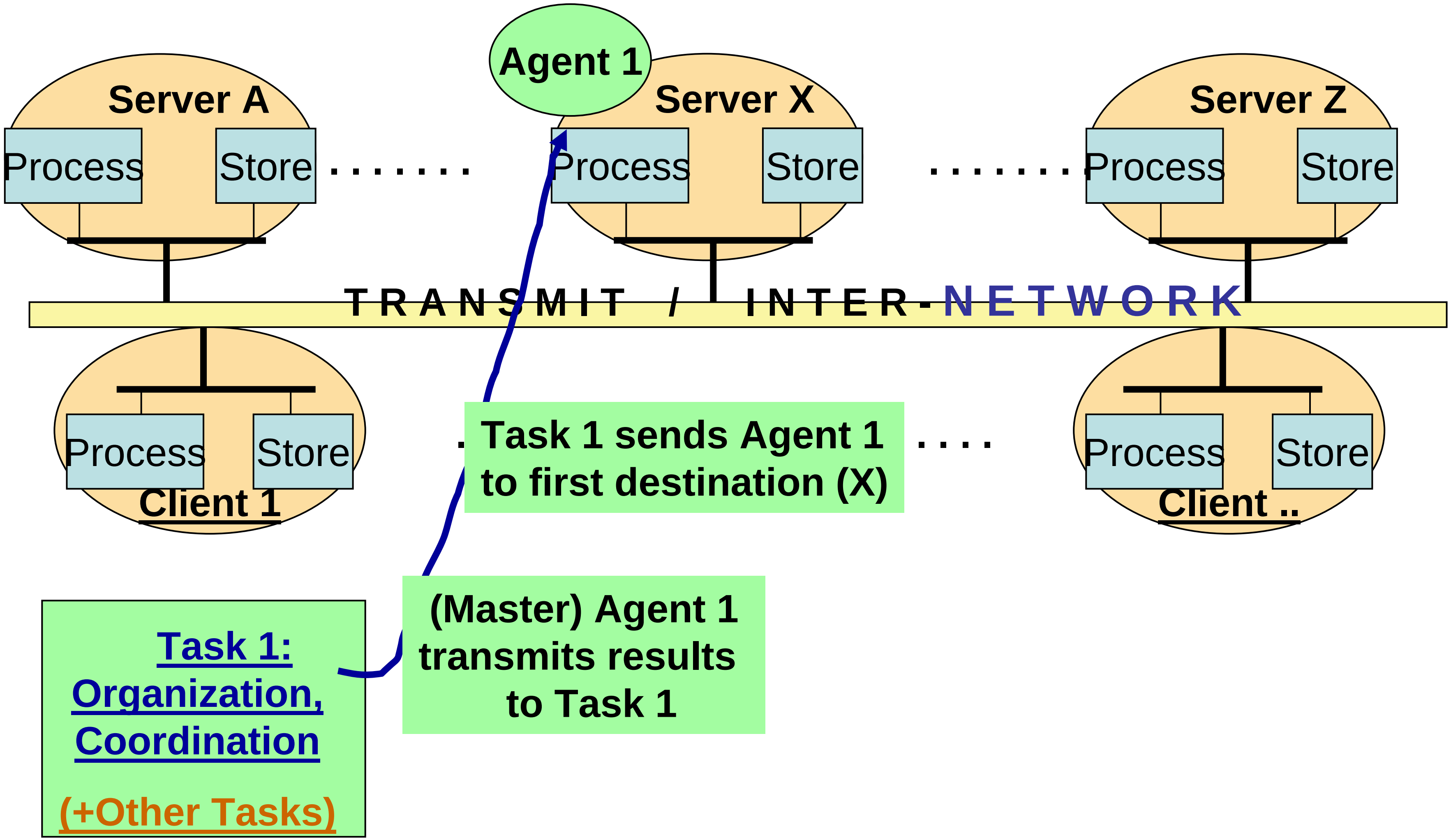
Evolution of System view of „Net-Work“:

From von Neumann´s EDVAC to „Ubiquitous Computing“:



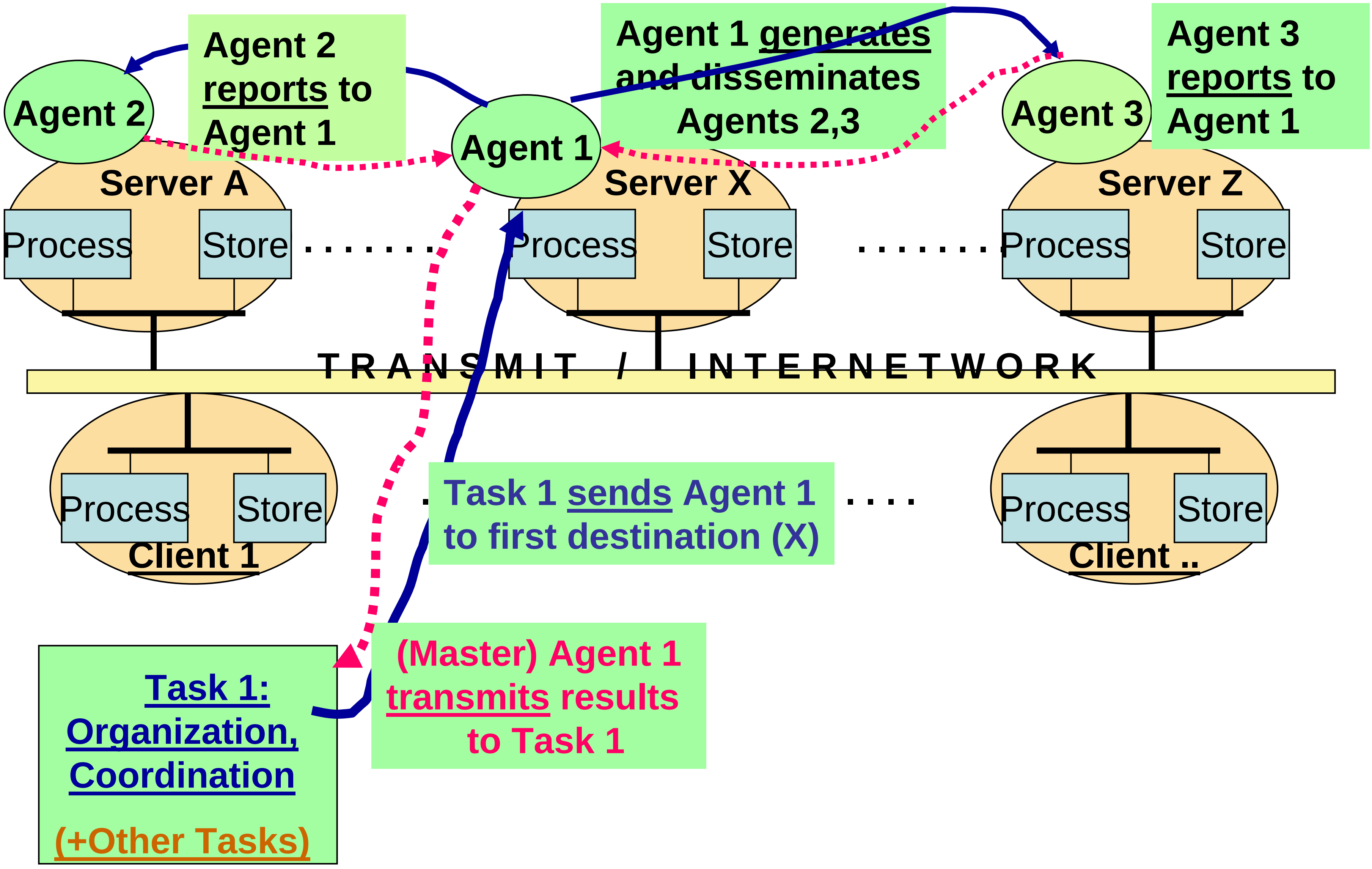
1.1j2 Phase 2 of The „Information Economy“

Distributed Architecture enables NetWork as Cooperation of Distributed Mobile Agents:



1.1j3 Phase 2 of The „Information Economy“

.... NetWork as Cooperation of Distributed Mobile Agents:



1.k Special Aspect: Moore´s Law: valid until?

- **From Intel´s present website:**

  Gordon Moore made his famous observation in 1965, just four years after the first planar integrated circuit was discovered. The press called it "Moore's Law" and the name has stuck. In his original paper, Moore observed an exponential growth in the number of transistors per integrated circuit and predicted that this trend would continue. Through Intel's relentless echnology advances, Moore's Law, the doubling of transistors every couple of years, has been maintained, and still holds true today. Intel expects that it will continue at least through the end of this decade. The mission of Intel's technology development team is to continue to break down barriers to Moore's Law.

1.1k1 Beyond Stage 2 of the „Information Society“

Reaching Physical limits: **Moore´s Law (duplication of speed every 18 month) valid until atomic distance is reached: ~2020! (probably earlier: problems of heating and packaging) → end of 2nd K-cycle**

Consequently, Lead DTs of phase 3 will be based on other physical principles:

Candidate: „quantum computing“

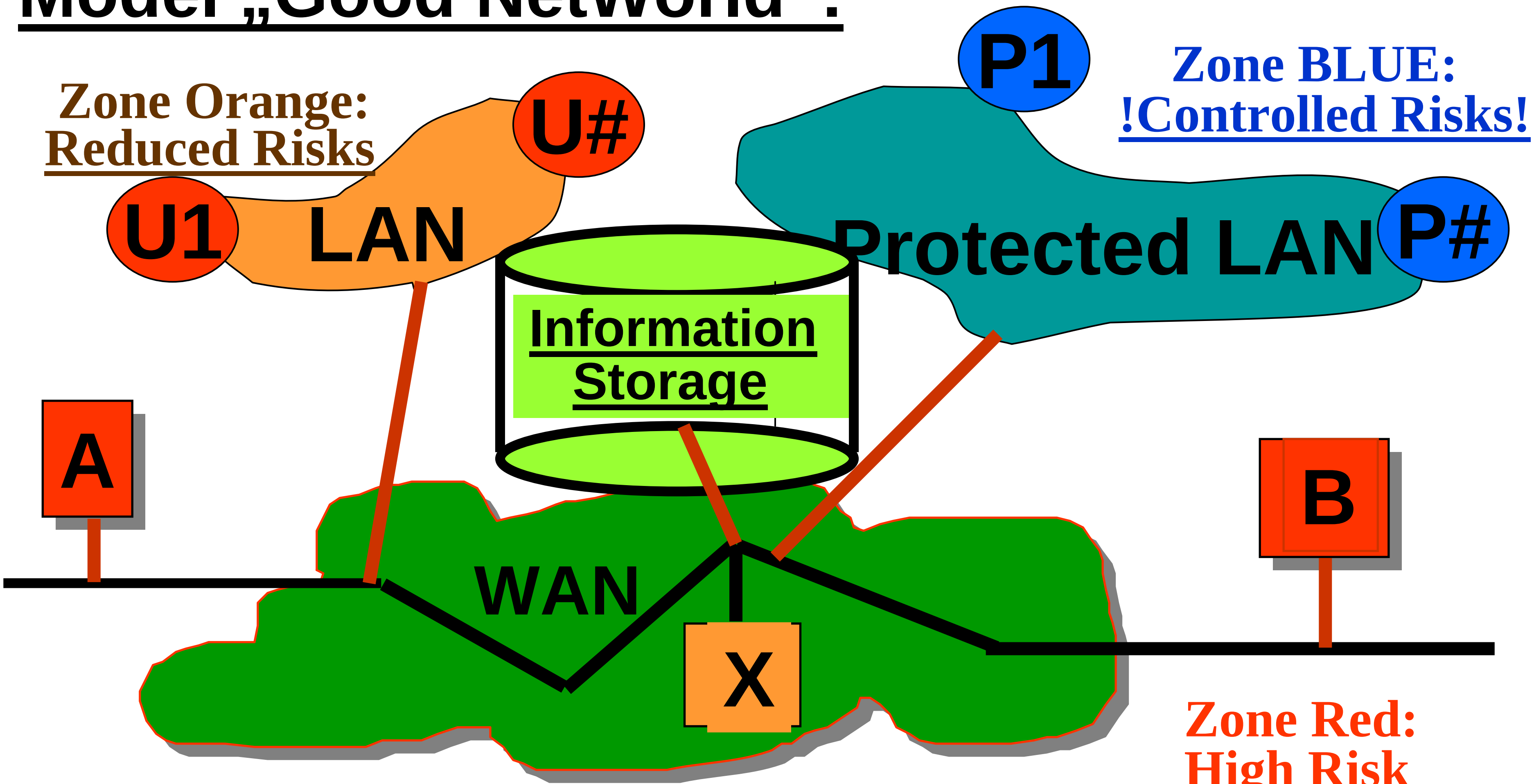
Problem: quantum logic is basically different from classical logic (used presently):

Classical Logic: „Tertium non datur“: (A) or (Not A)
→ Programming clause: „if (A) then ... else ...“

Quantum logic: (A) or (Not A) or (A AND NOT A)
→ Programming very different, and it is incompatible with contemporary programming.

1.1l Hopes: d- Enterprise use The Internet

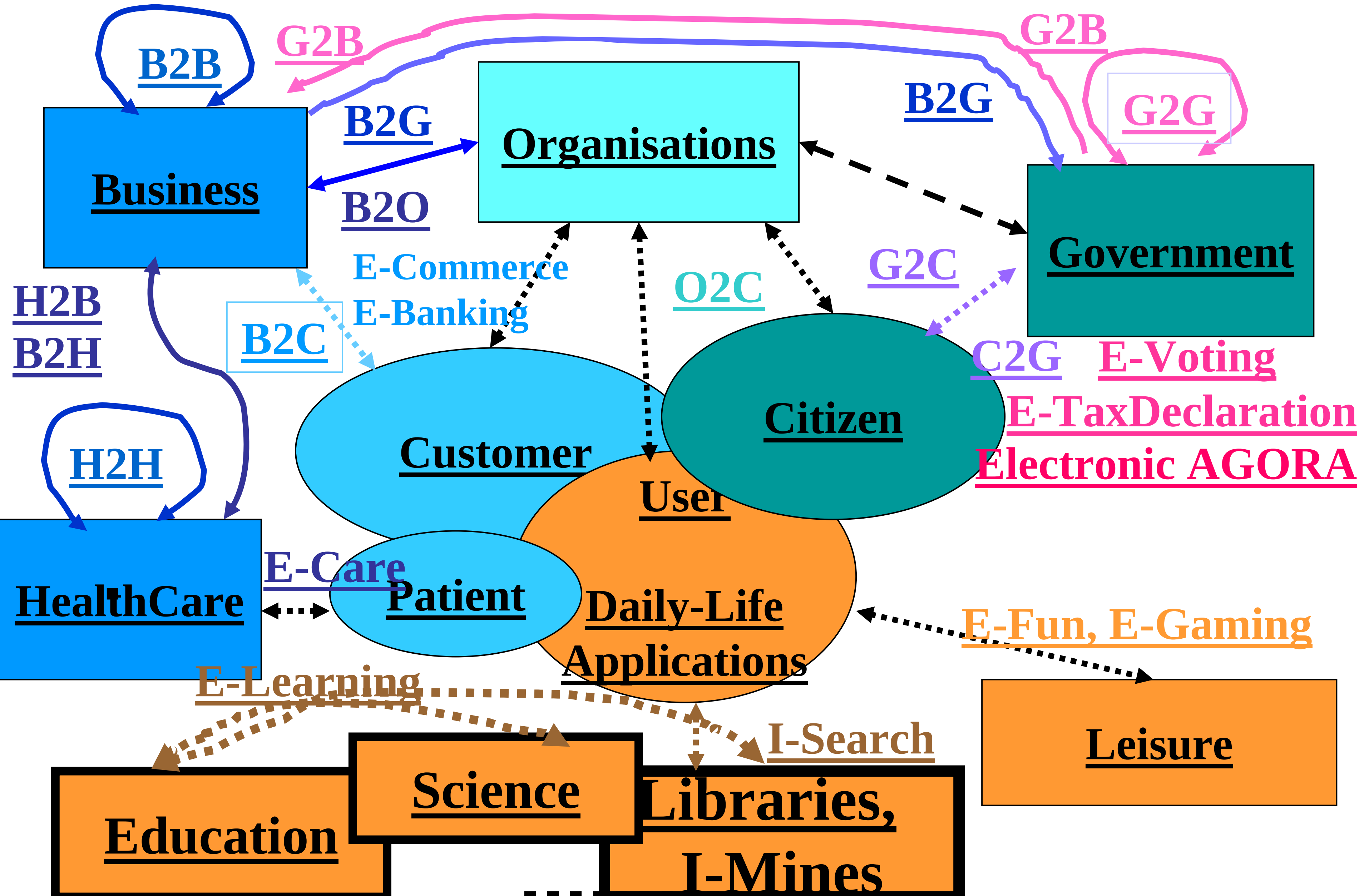
Model „Good NetWorld“:



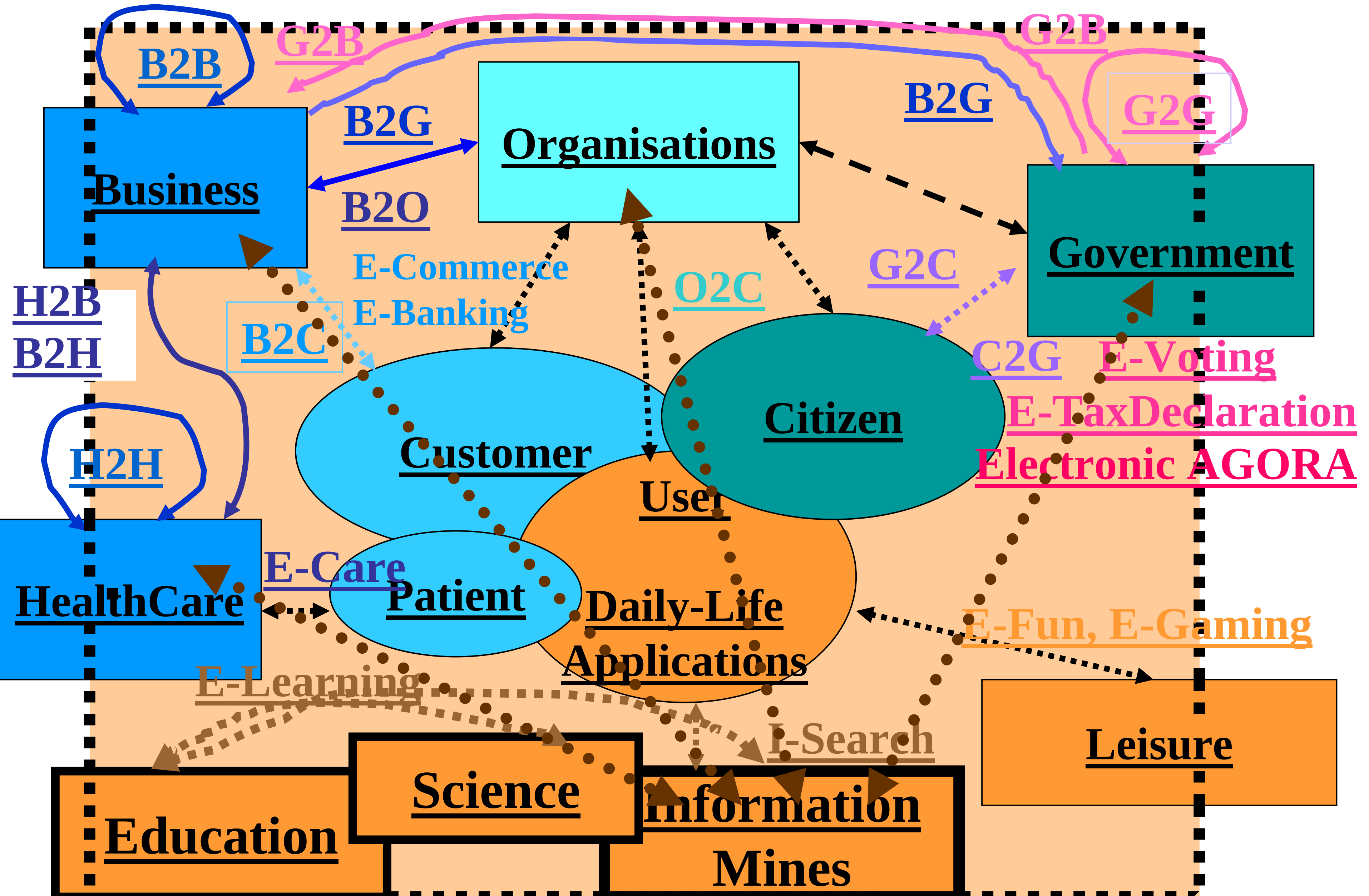
X: DoSomething

WAN =Wide Area Net

1.2a General Interactions in the Information Society:



1.2b Example „Information Mining“:



1.2b1 Case „Information Mining“ as „Exploitation“:

Digital Relation Business – Customers:

FROM: customer care (processing contracts, support)

TO: multiple customer profiles used for risk analysis, e.g. banks, insurance (car, health)

Digital Relation Government – Citizen:

FROM: citizen support (inhabitant, services, …)

TO: uniform organisation of public databases, including tax, police et al IS, enabling multiple filters („Raster“) (using uniform tax#)

2.0 Granular Structure of Digital Technologies

.1 Traditional Granularity: ISO/OSI model (7 levels)

.2 Refining Level 7: „Application level“, Risk Analysis

.3 Further Refinement: „Active Presentation“

2.1a Traditional Granularity: ISO/OSI model

Layer 7 – Application: **Provides network services to the end-users; Mail, ftp, telnet, DNS, NIS, NFS are examples of network applications.**

Layer 6 – Presentation (special meaning in network terms)

Layer 5 – Session ....

Layer 4 - Transport..........

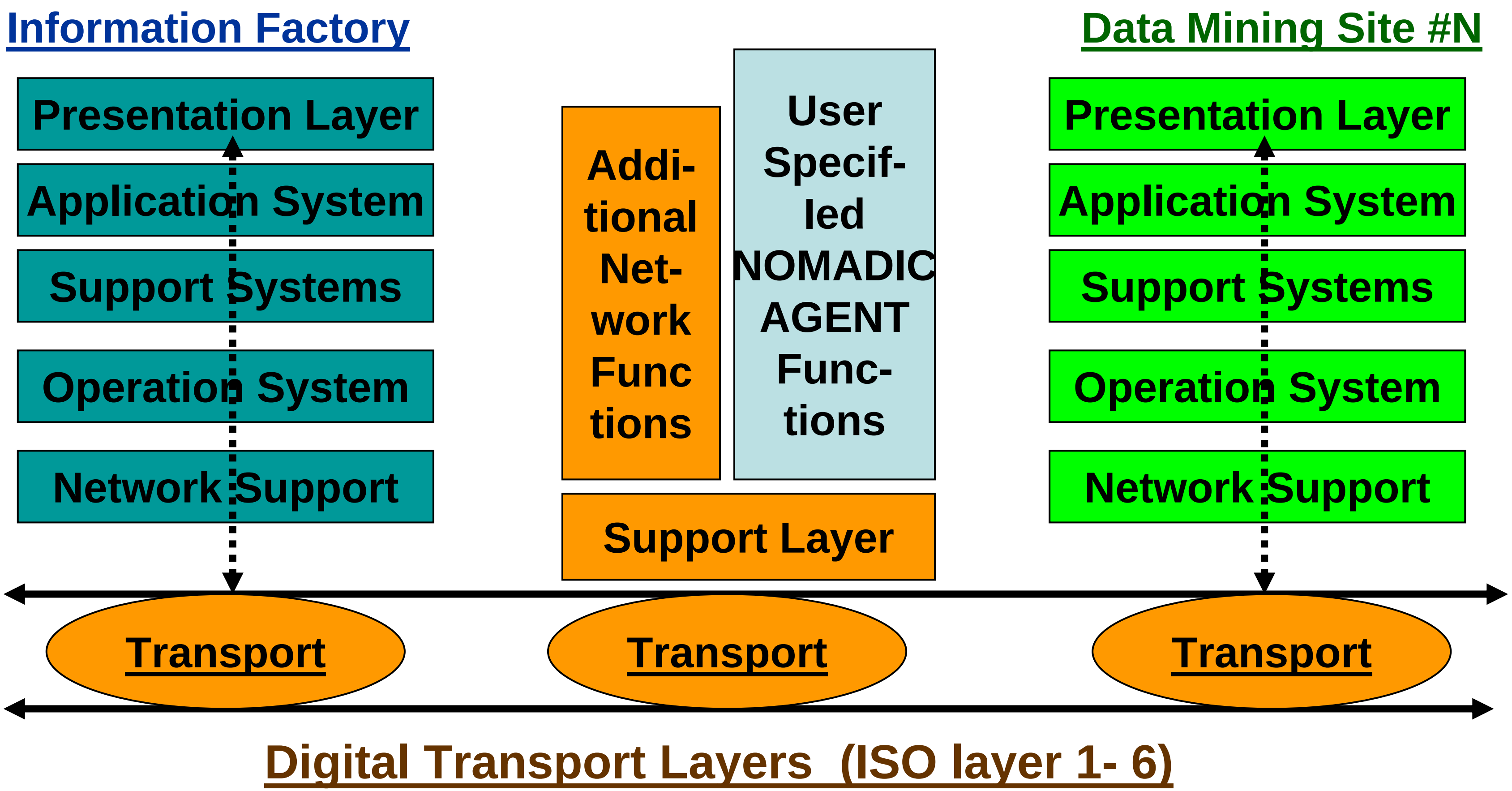
Layer 3 – Network ....

Layer 2 - Data Link..........

Layer 1 - Physical..........

Critical Comment: This model doesnot support requirements of „Information work". Instead of using standard services, users require that network services which can flexibly be connected to the „APPLICATIONS", with results visible on their „PRESENTATION" (aka screen).

2.2 a Fine Structure of Level 7: „Application level“



Example: User sends agent searching for data. Agent install itself at NOMADIC SUPPORT SITE and searches data at mining site #1. Data are preprocessed and sent to user while agent continues searching.

2.2 b Fine Structure of Level 7: Risk Analysis

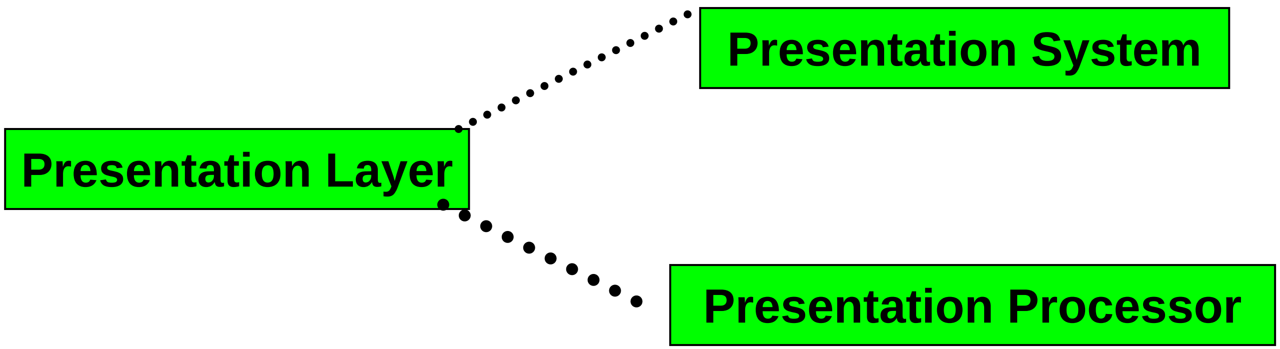
Security Risks:

Weak User Authenticity
Lost Functional Integrity
Lost Data Integrity
Unreliable Functions: exploits, ...
Undesired Functions: spyware, trapdoors ...
Denial-of-Service
Undercover Agent
Trust in Agent Lost
....

Digital Transport Layers (ISO layer 1- 6)

2.3a Further Refinement: „Active Presentation“

„Active presentation“ requires a <u>further refinement of the (hi-level) presentation layer</u>:



<u>Data part</u>

<u>Active part</u>

Embedded code, invocation of functions, URLs, ..

Hi-level interactive languages e.g. HTML, XML, ...

<u>Risk of „Active Presentation“:</u> when importing and activating an „active presentation“, user observes only data part (on screen), but can hardly observe effects of the „active part“!

3.0 Risk Analysis of emerging DTs

.1 Contemporary Risks

Survey of known risks

Newly emerging risks

.2 Symbian Mobile Phone Malware

State-of-Art

VTC detection test

.3 Emerging Risks from Harmful Active Content

„HTML (XML) regarded harmful“

3.1a Survey of Experienced Risks

Paradigmatic Risks:

Complex systems, difficult to understand

Interoperation of complex systems

Concept of „normalized relations“ without „renormalization“

Basic Concepts not used as specified:

Internet Protocol as conceived by Baran et al

HyperText Markup Language

Implementation Errors (bugs):

Inadequate implementation tools (languages, missing QA)

„Lazy“ programming techniques (Buffer Overflow, ...)

Inadequate Administration and Usage:

Essential Principles (4-eyes pr., minimum privileges) not applied

Missing user education and guidance

Missing surveyance leads to attacks: DDoS, Malware, ...

<u>3.1b Risks of Digital Complexity</u>

<u>Survey of architecture of contemporary systems</u>

<u>Presentation layer</u>: WYSIWIG
(What You See is What You)

O(100 MB)

<u>Application layer</u>

O(GB-TB)

<u>System Layer</u>: Organisation of resources (storage, processor, devices); problem solving (deadlocks etc); security services process support

O(1 GB)

Firmware, drivers

<u>Hardware layer</u>: processor, storage, bus; connections to devices and network

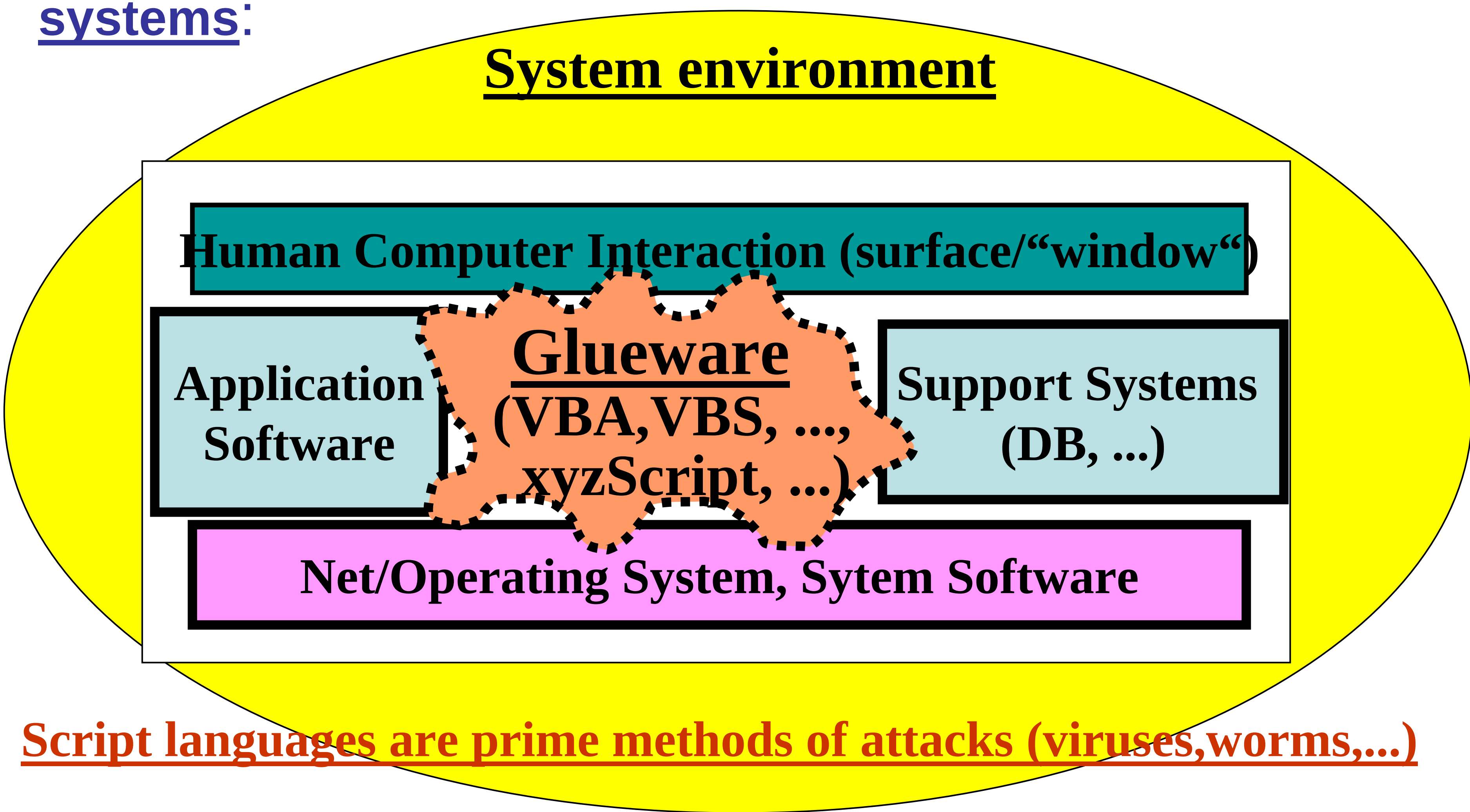
Bus

Net

<u>WYSIWYG principle does NOT hold (even for experts</u>

3.1c More Complexity through Interoperation

Script languages support interoperability of incompatible systems:

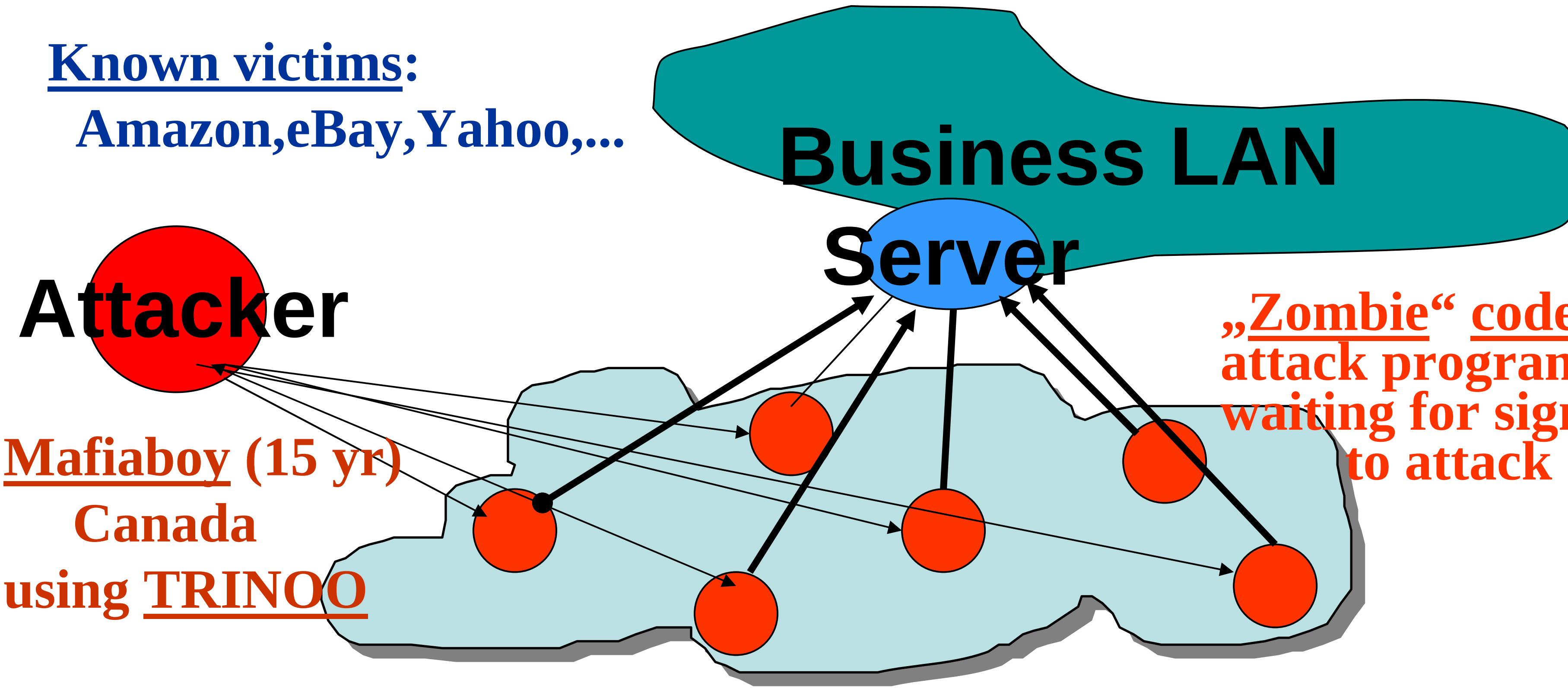


Script languages are prime methods of attacks (viruses,worms,...)

3.1d Risks of DDoS (Denial of Service Attacks)

Experienced DDoS attacks of February 2000:

Known victims:
Amazon,eBay,Yahoo,...

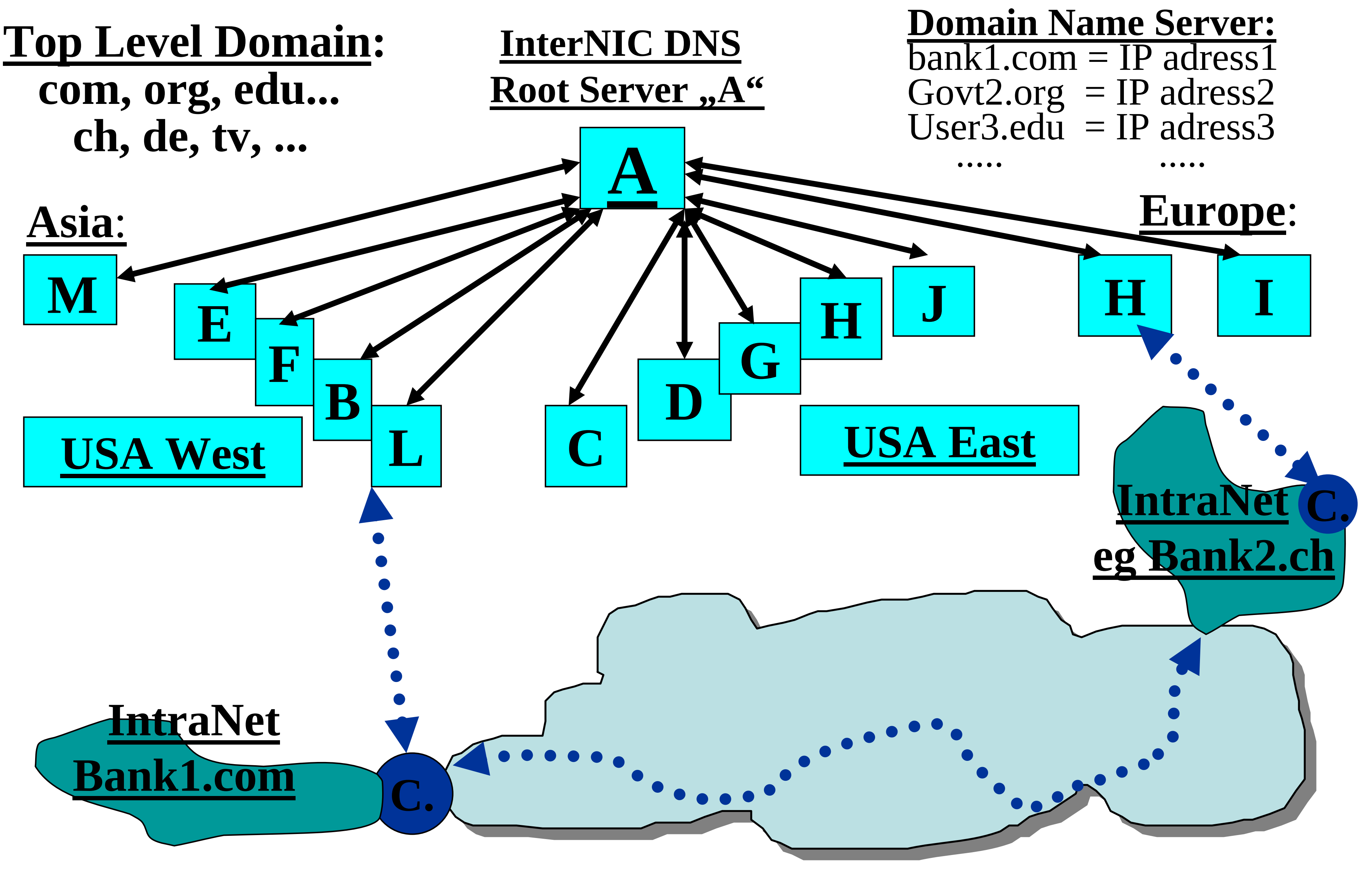


Mafiaboy (15 yr)
Canada
using TRINOO

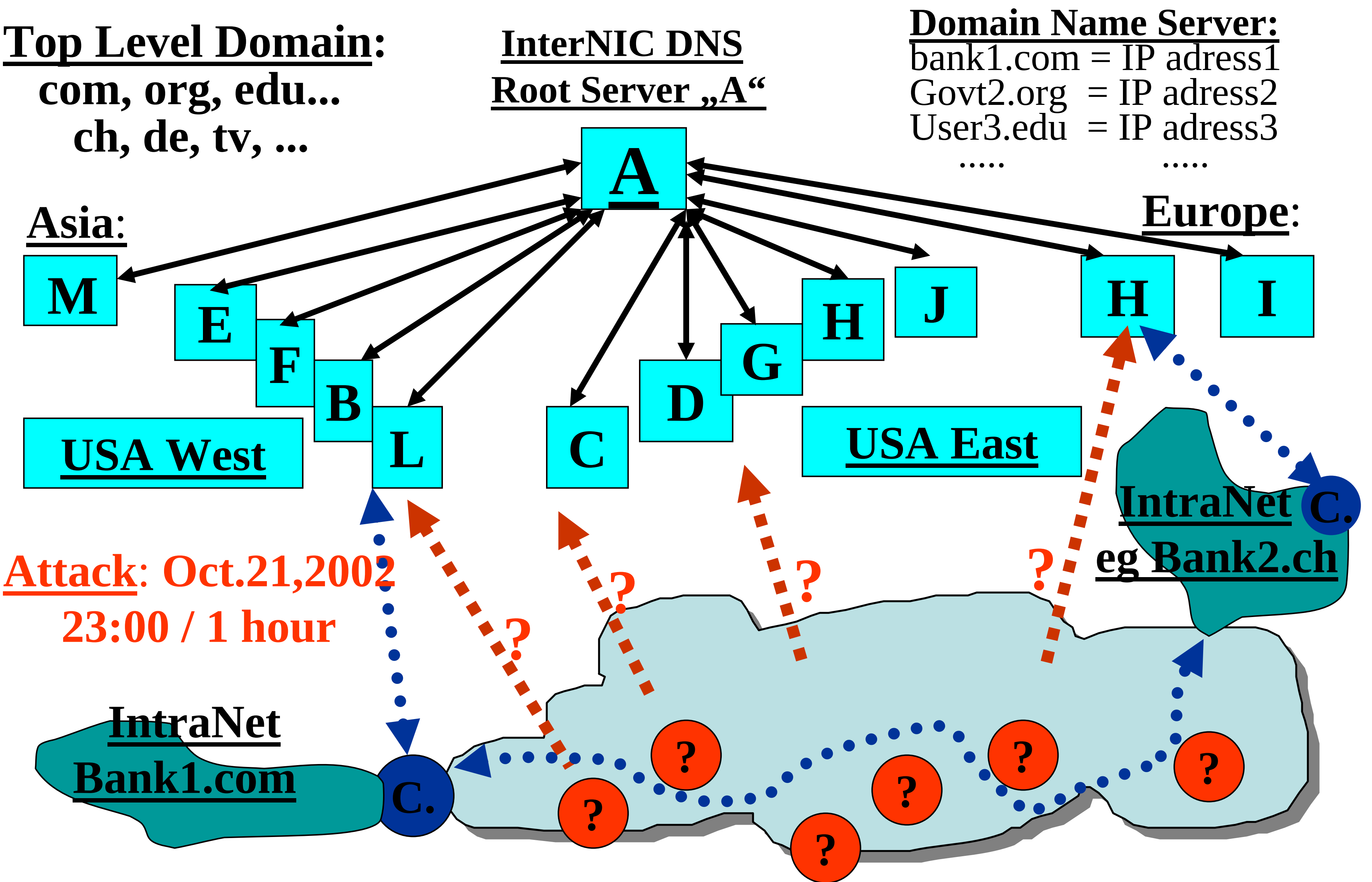
„Zombie“ code:
attack programs waiting for signal to attack

Attacker: deploys TRINOO, triggers attack

3.1e1 Combined Risk of Hierarchical DNS structure:

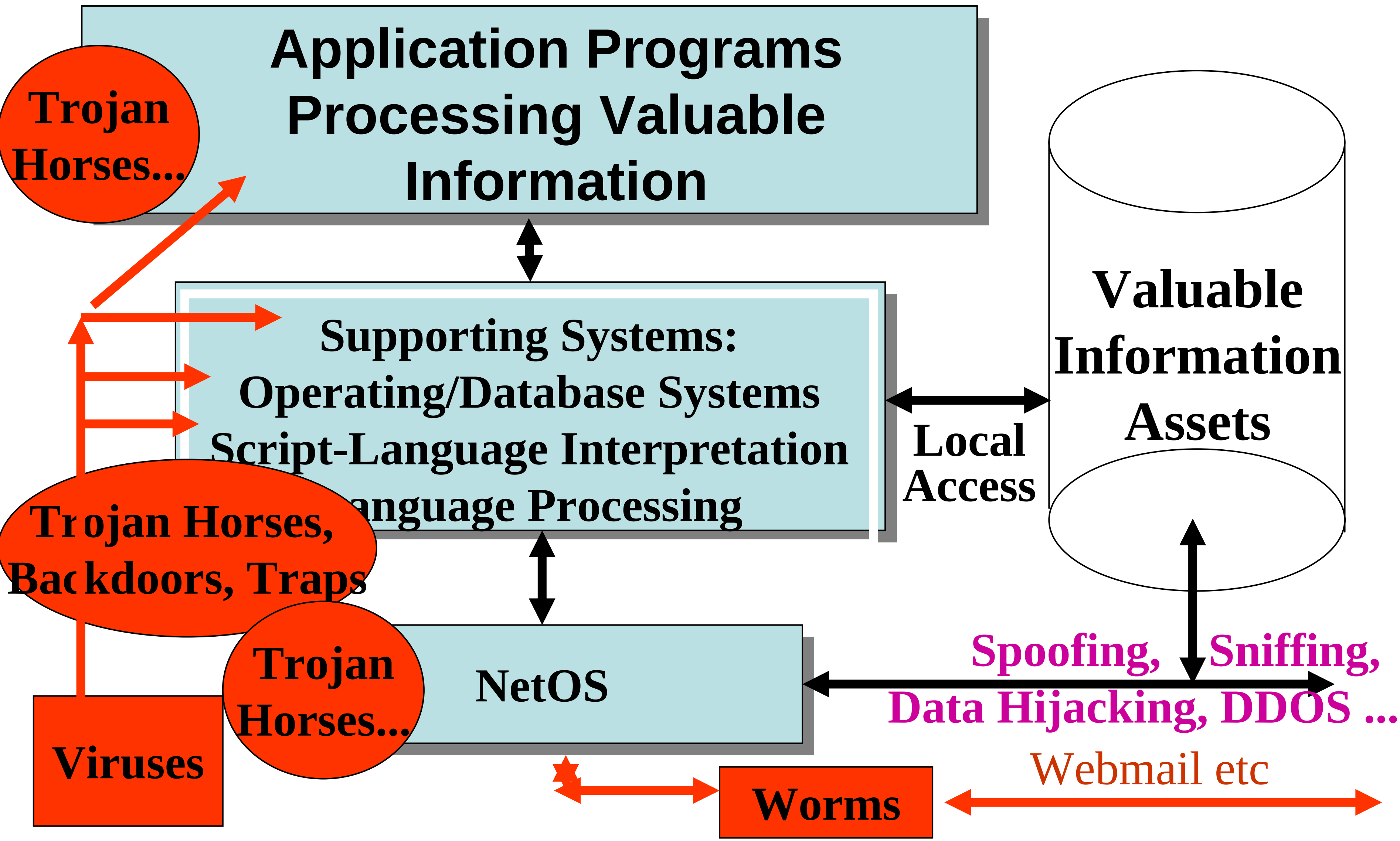


3.1e2 Combined Risk of Hierarchical DNS structure:



3.1f Digital Pandora´s „Malware Box“:

(approaching 300.000 specimen of malware)



3.1f2 Mechanisms for „FederalTrojan“ Operations:

Fact: trojans are used (PROVABLY) in multiple ways for **industrial espionage** (>150.000 samples of spyware) and (likely) for **government activities** (e.g. „agencies“).

Assumption: for legal purposes and under specific laws, known techniques may be used (under specific precautions such as judge permission) for fighting big crime and terrorism with some form of **„Online raid“** (using a category of adaptive „Bundestrojaner, BT“)

Methods for Installation of „BT“:

a) email with **inline code** (e.g. W97M) or **appended trojan,**

b) **penetration via covert channel** in application or system,

c) with **help of ISPs**: modification of information in transit (e.g. user requested downloads), or

d) with **help of system producers**: a **covert channel in system software**, enforced by law

Die Online-Durchsuchung ist da!

3.1f3 Mechanisms for FederalTrojan Operations (#2):

Methods for Detecting „BT“:

Even if adaptive (e.g. polymorphic), any BT may be detected (even as day-0 attack) with contemporary behaviour based protection software (IDS, AV/AM, FW).

Methods for Avoiding „BT“:

As installation requires related permission, installation may be blocked with contemporary change supervisors (except when suitably patched systems circumvents such software.

Usage of data (evidence) gathered by „BT“:

Even if related data are successfully collected and exported, it is questionable whether these data can be used as EVIDENCE in court (e.g. it must be excluded that the data may have been produced by the „forensic software“ itself).

3.1g1 Attacking e-Banking: Website as Relay

From: Deutsche Bank [BrandvoldClifford@deutsche-bank.de]
Sent: Sonntag, 29. Mai 2005 04:14
To: brunnstein@informatik.uni-hamburg.de
Subject: Deutsche Bank Email Verification - brunnstein@informatik.uni-hamburg.de

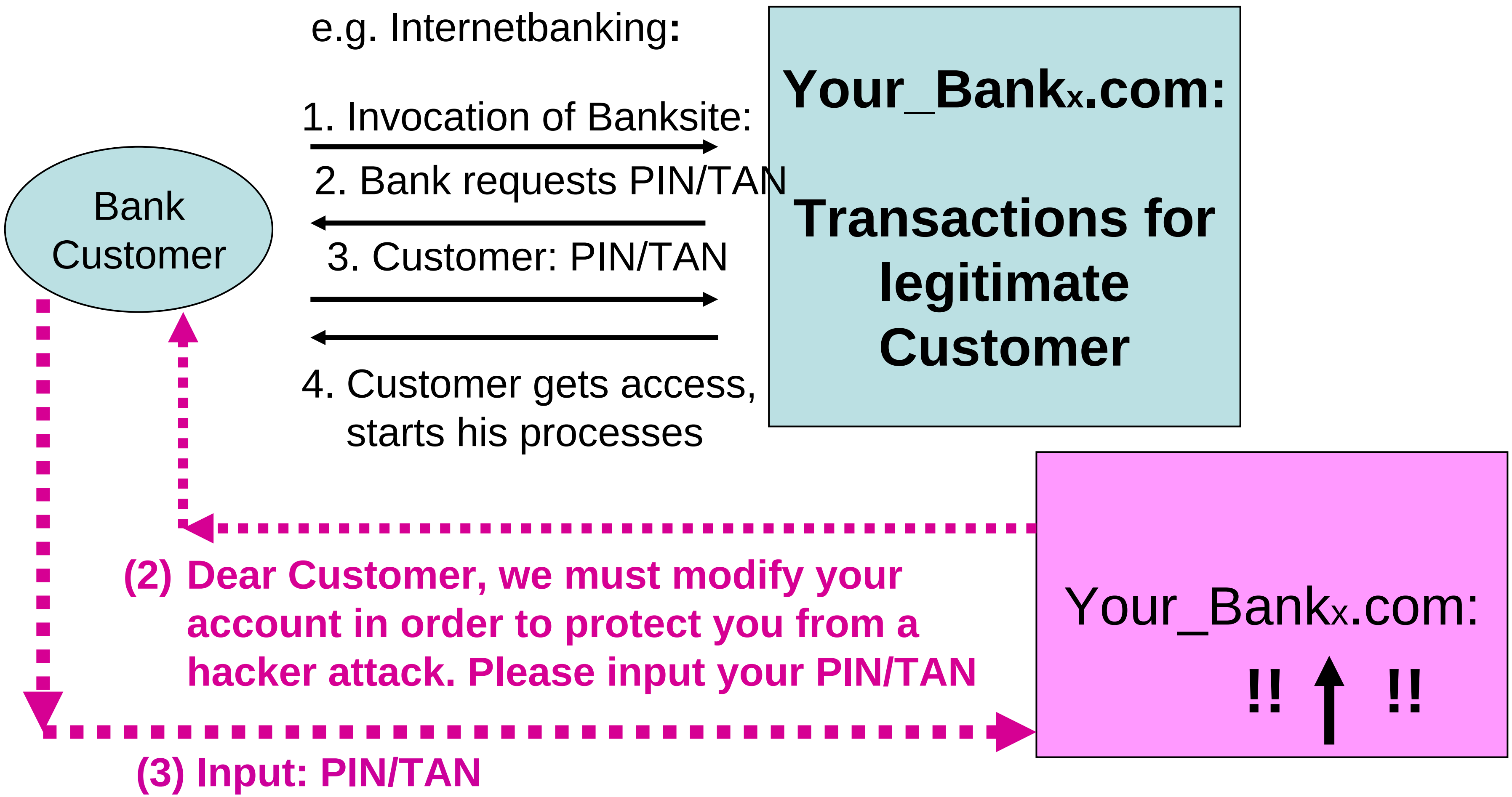
Dear Deutsche Bank Member,

This email was sent by the Deutsche Bank server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your Deutsche Bank online access details. This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it. To verify your e-mail address, click on the link below:

http://www.deutsche-bank.de
/AMsChXxJv1oQh4JbrhrtoZdSgbH3llhObxxnUkV7zAEwMhrmzA0f2cf6d03v

3.1g2 Attacking e-Banking: Phishing

„Phishing“: a malicious method to access sensitive data (e.g. bank accounting)



3.1g3 Attacking e-Banking: „Pharming“

Attack first observed in March 2005:

The „normal“ URL

„Your_Bank.com“

can also be the ASCII representation of some URL written in other character sets, such as Kyrillic or Greak. While such URLs differ in their Unicode representation, browsers will normally only be able to present their ASCII instantiations. This URL leads to a different IP adress than the bank´s one (Technique called „DNS Poisoning“).

Countermeasure: Browser option to present only ASCII characters.

3.2a Symbian MobilePhone Malware: Threats

Advent of Mobile Malware:

- Platforms (Symbian, EPOC, ...) conceived to support easy implementation of applications
- Programming in script languages, no exclusion of potentially harmful functions
- Example: platform = Symbian OS
  - **Presently known: 12 different strains (families) of self-replicating (=viral) or not self-replicating (=trojanic) malware with 100 variants or modifications**
  - **Malicious functions: most specimen are „proof-of-concept“ malware (viruses/trojans) but some have a dangerous payload**
  - **Example of dangerous payload:**
    - **Reorganize dictionary of telephone numbers**
    - **Send MMS to every entry in telephone dictionary (real „payload“ ☺)**

3.2b Symbian MobilePhone Malware Test: Products

14 Products in aVTC test: (versions: May 2005)

ANT	AntiVir (H&B EDV)	(Germany)
AVA	AVAST (32)	(Czech Republic)
AVG	Grisoft Antivirus	(Czech Republic)
AVK	AntiVirus Kit (GData)	(Germany/Russia)
AVP	AVP (Platinum)	(Russia)
BDF	BitDefender (AntiVirus eXpert)	(Romania)
FPW	FProt FP-WIN	(Iceland)
FSE	F-Secure AntiVirus	(Finland)
IKA	Ikarus Antivirus	(Austria)
MKS	MKS_vir 2005	(Poland)
NAV	Norton AntiVirus/Symantec	(USA)
NVC	Norman Virus Control	(Norway)
SCN	NAI VirusScan/McAfee	(USA)
SWP	Sophos AntiVirus (Sweep)	(UK)

3.2c Symbian MobilePhone Malware Test: Testbed

Testbed (all specimen known May 12, 2005):

Cabir	22 Variants (a ... .v),
	1 dropper (installing variants .b, .c, .d)
Commwarrior	2 Variants (a-b)
Dampig	1 Variant (a)
Drever	3 Variants (a-c)
Fontal	1 Variant (a)
Hobbes	1 Variant (a)
Lasco	1 Variant (a)
Locknut:	2 Variants (a, b)
Mabir	1 Variant (a)
MGDropper (Metal Gear trojan)	1 Variant (a)
Mosquitos	1 Variant (a)
Skulls	11 Variants (a-k);
	52 modifications of Skulls.D

12 strains (=„families“) with 100 variants/modifications.

3.2d Symbian MobilePhone Malware Test: Results

Rank/Product		Detected (135 samples)	DetectionRate(%)	Grade
(6)	ANT	92	68,15	Risky
(6)	AVA	53	39,26	Risky
(6)	AVG	119	88,15	Risky
(2)	AVK	131	97,04	Very Good
(1)	AVP	134	99,26	Excellent
(4)	BDF	126	93,33	Good
(13)	FPW	13	9,63	Inacceptable
(2)	FSE	132	97,78	Very Good
(6)	IKA	57	42,22	Risky
(6)	MKS	55	40,74	Risky
(6)	NAV	81	60,00	Risky
(13)	NVC	5	3,70	Inacceptable
(4)	SCN	123	91,11	Good
(6)	SWP	60	44,44	Risky

3.3 Emerging Risks from Harmful Active Content

Risk applicable to Application level: Programming malicious software made easy:

Hi-level interactive (=interpretative) programming languages:

- **(Visual) BASIC dialects**
- **Other Script languages (SAPscript ...)**
- **JAVA (if JVM running on-top of another operating system, sandbox can be attacked from „down-under")**
- **Markup Languages (MLs): HTML, XML, ...**

Risks of HTML (as presently used, NOT as designed!):

- **execution of active content embedded/hidden in object**
- **references (URLs) outside document may import unknown content**
- **import of objects of various formats, implying application of processors of unknown quality and interoperability**

4.0 Approaches to safe and secure DTs

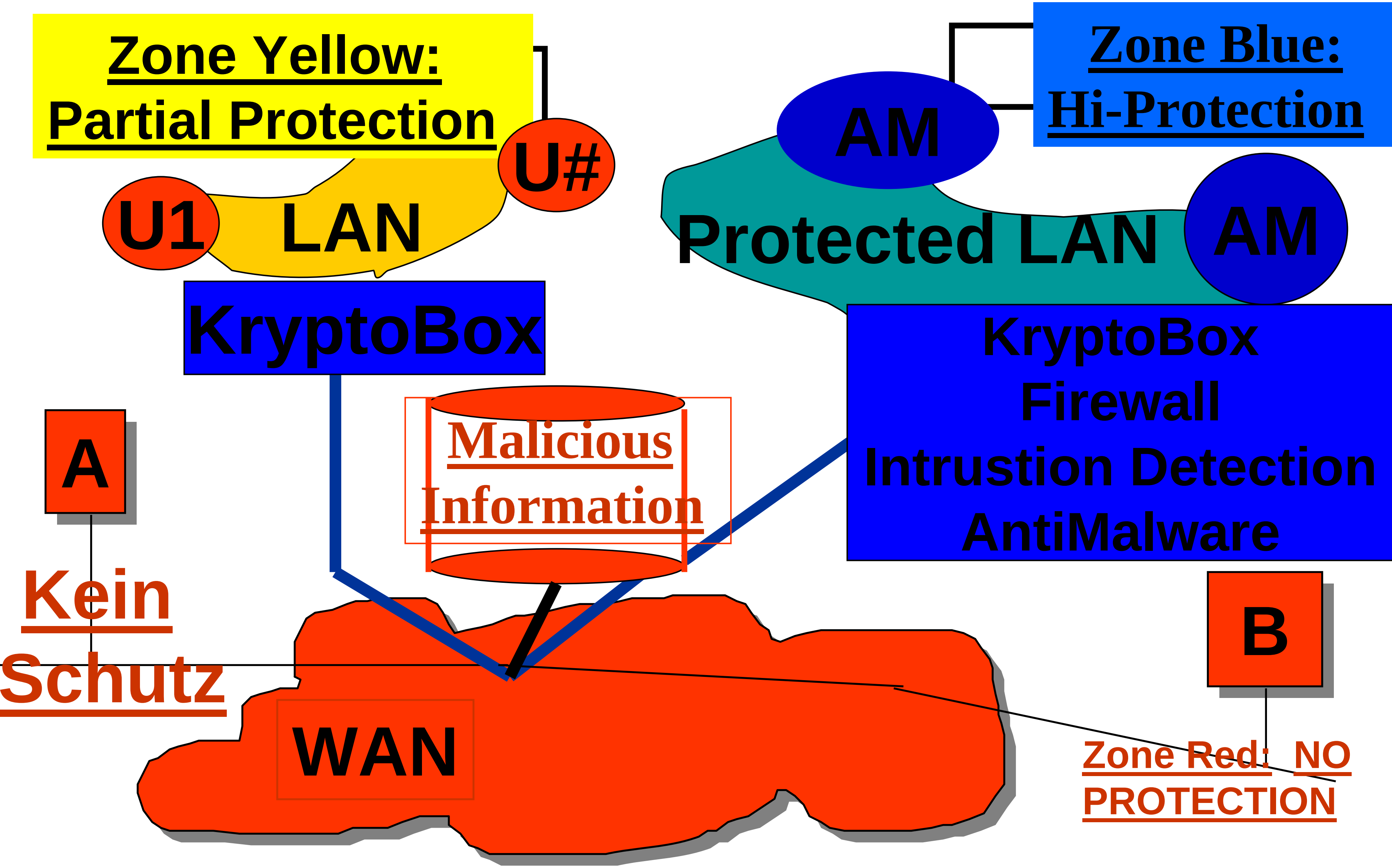
.1 Contemporary Solution: „Tower of IT“

.2 Requirements: Inherent Safety & Security

.3 Residual Technical Risks

.4 (Legal) Enforcement

4.1 Contemporary Solution: „Tower of IT“



4.2 Requirements for Inherently Safe&Secure Systems

Basic requirement: for all IT systems in a ubiquitous network (including devices in personal contact), manufacturers specify and guarantee essential functions and features.

Requirement #1: „SafeComputing“ (SC):

SC architecture guarantees: functionality of processes, persistence & integrity of objects, encapsulation of processes, graceful degradation (!), benign recovery (!)

Requirement #2: „SecureNetworking“ (SN):

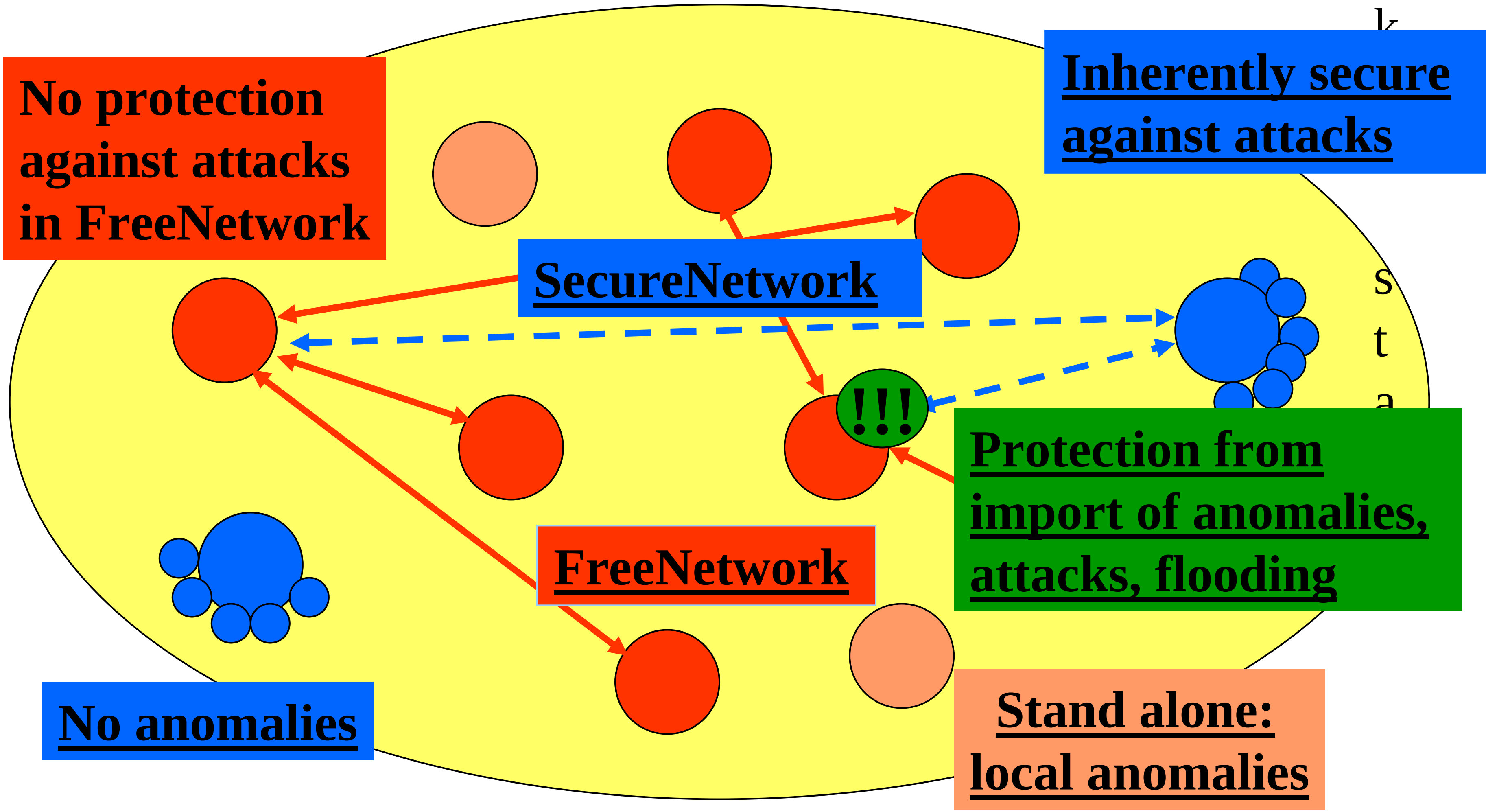
SN protocol guarantees: confidentiality, integrity, authenticity of sender/receiver, reliability of transfer, non-repudiation (!), non-deniability (!)

Requirement #3: Assurance of functional adequacy:

All functions and features must be specified and implemented in a way to permit adequate assurance of specifications.

4.3 Residual Risks in Ubiquitous Computing

Future Secure and InSecure Networlds:



4.4 Enforcement of Inherent Security

Path #1: DT Manufacturers establish and enforce adequate quality and standards.

- **Example: Vapor engine quality enforced through „Dampfkessel Ueberwachungs-Verein“ (now: TÜV)**
- **Presently, no such self-organisation of ICT industry is available.**

Path #2: Directives (EU, president) and laws enforce protection of customers (persons AND enterprises), including damage compensation and preventive actions.

- **Example: customer protection legislation in USA etc followin Nader´s book „Unsafe at any speed!“**