ASQF

Arbeitskreis Software-Qualität
und Fortbildung e.V.
FG Software-Test Norddeutschland, Bremen
und

Gesellschaft für Informatik
Regionalgruppe Bremen Oldenburg

Hochschule Bremen 12. April 2011

"Aktuelle Angriffe auf industrielle Infrastrukturen (am Beispiel von Stuxnet)"

Dr. Klaus Brunnstein (Fellow GI)

Professor em. für Anwendungen der Informatik

Universität Hamburg

Präsident (2002-2007) Welt Informatik Organisation

IFIP (International Federation for Information Processing)

Abstract

Wie kritisch Unternehmen und die Wirtschaft insgesamt vom sachgerechten Funktionieren wichtiger industrieller technischer Infrastrukturen abhängen, wird seit Beginn des Industriezeitalters durch zahlreiche Unfälle deutlich, insbesondere wenn deren Wirkungen nicht nur die Existenz der betroffenen Unternehmen, sondern ganze Regionen (etwa beim Reaktor-Unfall in Chernobyl) oder Wirtschaftszweige (etwa bei Unfällen der Ölproduktion) betreffen. Während die Verletzlichkeit von Netzwerk- und Bürosystemen durch zahlreiche Berichte über Hacker-Angriffe bis hin zum Kanzleramt hinreichend bekannt sind, ist bisher die Tatsache weniger ins Bewußtsein der Öffentlichkeit gelangt, dass Unternehmen und Volkswirtschaften in noch höherem Maße von I&K-Techniken abhängen, die sich mangels ausreichender Sicherheitsvorkehrungen allzu oft als anfällig für fehlerbedingte Ausfälle bis hin zu externen Angriffen erweisen.

Jüngst haben Berichte über die Infektion von zahlreichen Steuerungsrechnern von industriellen Produktionsanlagen weltweit mit dem sog. "STUXNET-Virus" sowie dabei Vermutungen über Angriffsziele (vor allem Urananreicherungsanlagen im Iran) nachgewiesen, wie anfällig selbst vermeintlich aufwendig "gesicherte" Anlagen gegen Angriffe und Ausfälle sind. Solche Angriffe, die übrigens seit den 1990er Jahren mit der zunehmenden Vernetzung industrieller Anlagen beobachtet (wenn auch nich berichtet) werden, lassen eine Vielzahl an Motiven und professionellen Qualifikationen erkennen, während Abwehrmaßnahmen weder sachgerecht konzipiert und implementiert noch getestet und regelmäßig geübt werden. Diese Probleme werden zusätzlich überlagert über Spekulationen, dass Regierungen sich tatkräftig mit Angriffen auf staatlichen und industrielle Netze - "Cyberwar" - beschäftigen.

Ausgehend von einer kurzen Darstellung ausgewählter Unfälle industrieller Anlagen seit den 1990er Jahren wird die Verletzlichkeit bestimmter Produktionssteuerungsanlagen anhand des STUXNET-Virus erläutert, und dazu werden geeignete Vorsorge- und Schutzverfahren vorgeschlagen.

Der Stuxnet-Vorfall hat verschiedene Regierungen für Risiken von Cyber-Angriffen sensibilisiert. Der Vortrag stellt dazu Ansätze zur Gegenwehr in Deutschland, USA und Indien vor.

Aktuelle Angriffe auf industrielle Infrastrukturen
(dargestellt am Beispiel von Stuxnet)

1) Einordnung: Auf dem Wege zu Enterprise 3.0
2) SCADA: Supervisory Control and Data Acquisition
3) Angriffe auf industrielle Anwendungen
4) STUXNET: Technische Grundlagen, Angriffsmethoden
5) STUXNET: Zwischen Erkenntnis und Spekulation
6) Cyberangriffe und Gegenmassnahmen (D , USA, IN)

1.1 Phasen (1- 4) der „Industriellen Ökonomie“ (~) 50 Year Cycles

- **Schumpeter, Kondratieff:**

  Modell der industriellen Entwicklung, ausgearbeitet für die letzten beiden Phasen (Anbieter-getriebene Märkte)

- **Nefiodov: Modell angewandt auf Computertechnologien für die Phasen** 1-2:
  - **Phase 1** (1760+): Dampf-getriebene stationäre Maschine (externe Verbrennung)
  - **Phase 2** (1810+): Dampf-getriebene mobile Maschine

  → **Paradigmatischer Wandel der Leit-Technologien: from external to internal energy conversion!**

  - **Phase 3** (1860+): Öl-getriebene Maschinen (interne Verbrennung)
  - **Phase 4** (1910+) Elektrisch getriebene Maschinen, Netze

  ➔ **Vorbedingung für I&K-Technologien!**

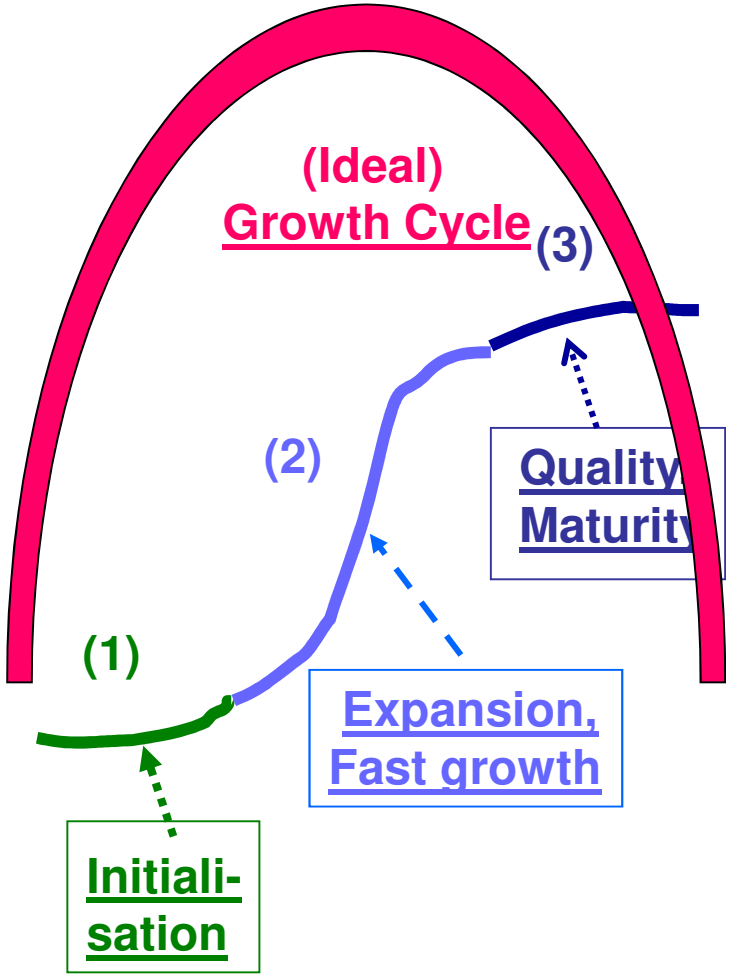
1.2 Phasen eines Kondratieff-Zyklus:

Paradigm of Kondratieff cycles:

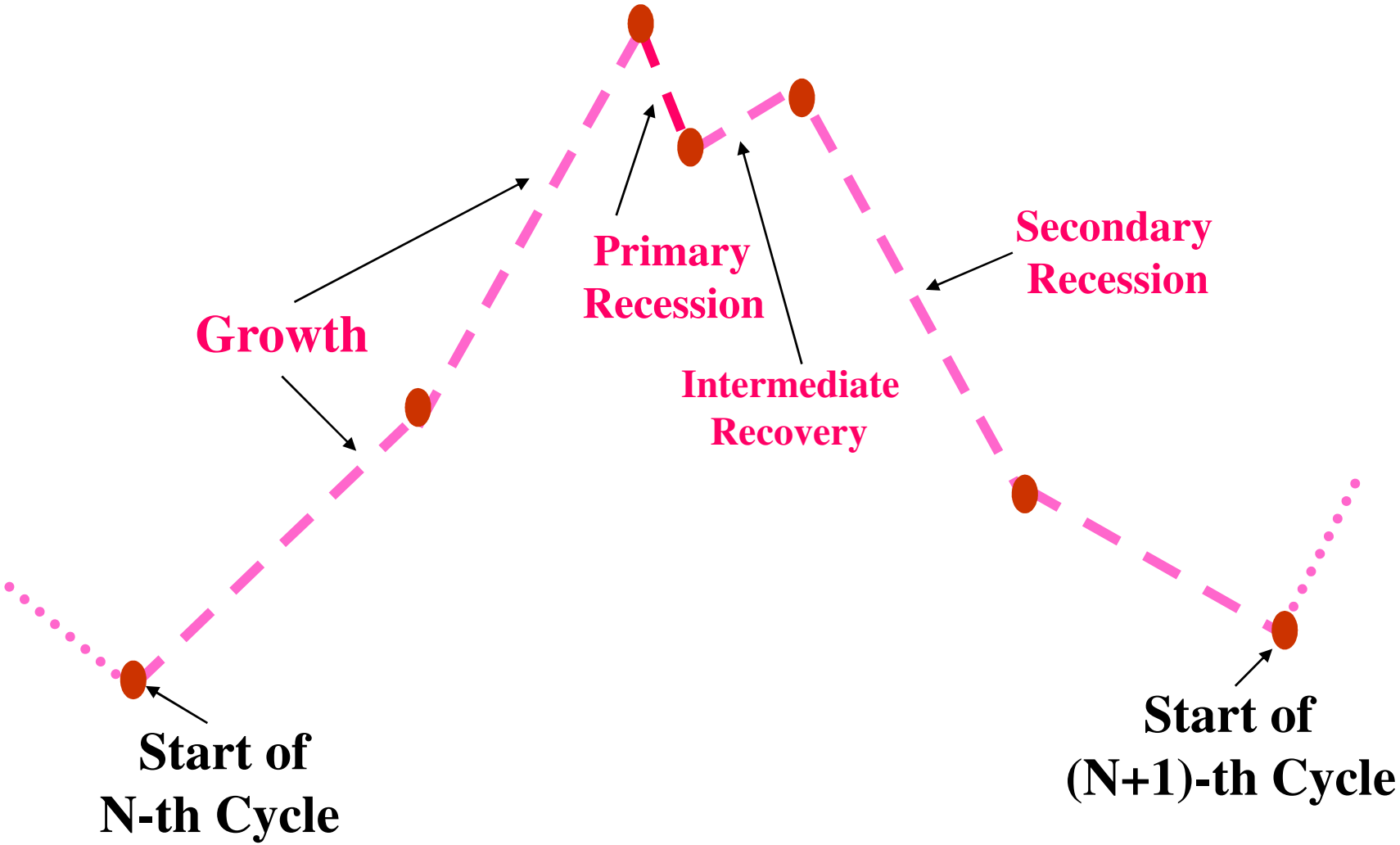
A „Lead (=Key) Technology“ has the power to induce a development cycle (about 40-50 years), with the following phases:

- (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“.

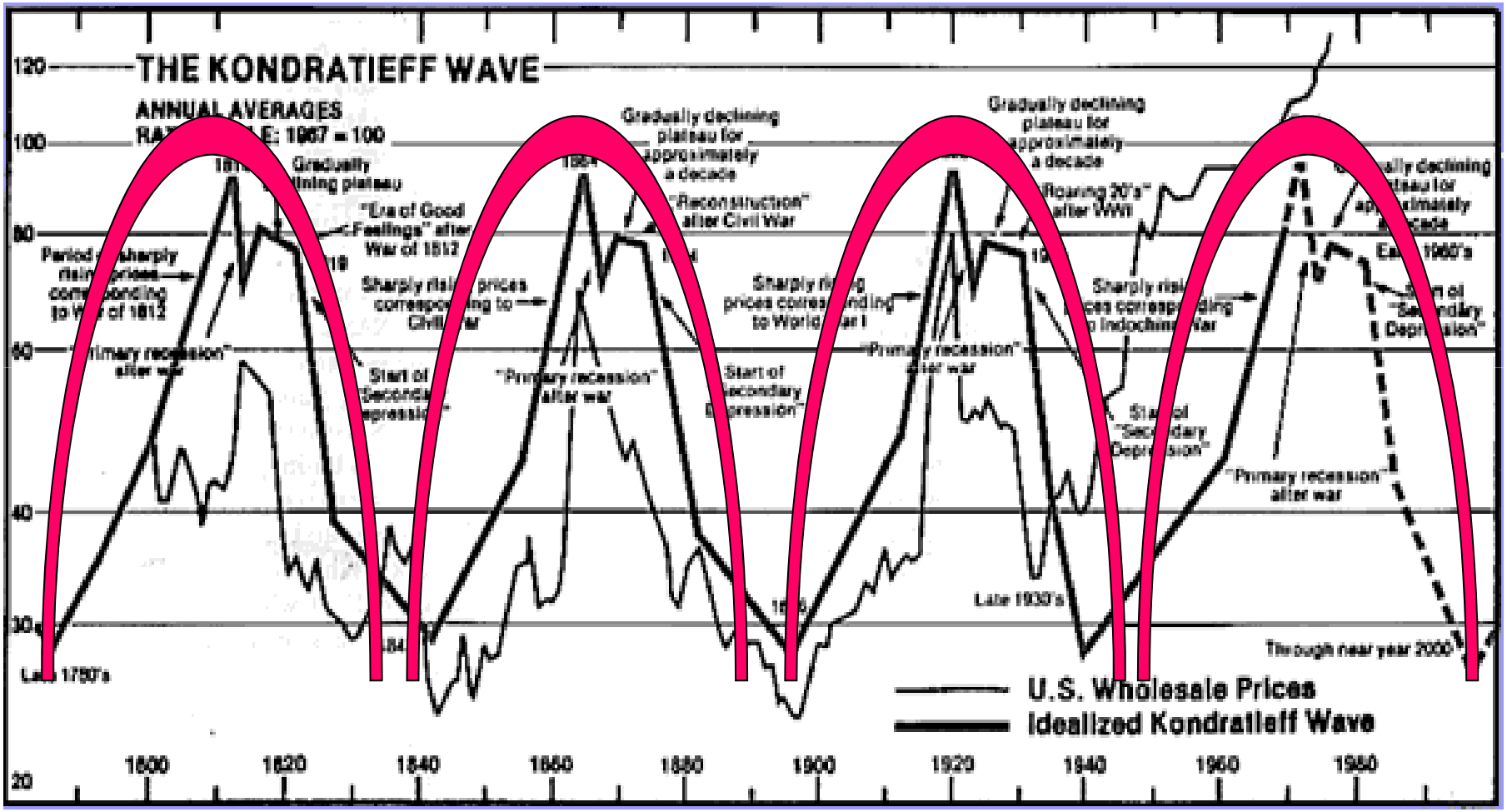
As this technology is „exhausted“ after phase 3, another lead technology will have to start shortly before the end of phase 3.



1.2a Feinstruktur eines Kondratieff-Zyklus:



1.3 Kondratieff: Leittechnikzyklen der Industriegesellschaft:



1814 1864 1920 1970

1.4 Zur Entwicklung der I&K-Techniken: Phasenmodell

Technische Leittechniken der Informationsgesellschaft:

1. Phase (1940-1990): Lokale digitale Systeme

Analogie: 1. Phase Industriegesellschaft: **ortsfeste Dampfmaschine**

- **Hardware**: Mainframe->Mini-Computer->Personal-Computer
- **Netztechnik**: lokale Verkabelung -> Telefon ... Satellit
- **Software**: Lokale Betriebssysteme: stand-alone ... DFÜ
- **Einsatzart:** I&K unterstützt tradierte Geschäftsprozesse
- **Anwendungen**: Software für feste Anwendungen: **O(MegaByte)**
- **Datenmengen**: Dateien -> Datenbanken: **O(Mega-GigaByte)**
- **Benutzer**: ausgebildet (Admin, Operateure, ... Benutzer)

2. Phase (1980-2020): Mobile digitale Systeme =„Agenten“

Analogie: 2. Phase Industriegesellschaft: mobile Dampf-Lokomotive

- **Hardware**: Verteilte Hardware, Server/Client-Architektur
- **Netztechnik:** LAN/MAN/WAN: Glasfaser ... Mobilfunk
- **Software**: Verteilte kooperierende Netz-Betriebssysteme
- **Einsatzart**: Geschäftsprozesse an I&K-Bedürfnisse angepasst
- **Anwendungen**: Software an vielen Stellen: **O(Giga-TeraByte)**
- **Datenmengen:** Verteilte „Warehouses“: **O(Peta-ExaByte)**
- **Benutzer**: abnehmende Ausbildung, jeder „macht alles selbst“

1.5 Zur Entwicklung des IKT-Einsatzes in Unternehmen: Von Mainframes zu Enterprise 3.0:

Zur Einordnung: Ein kurzer Abriss des Zeitablaufes

Phase 1 (1960+): Zentralisierte IT-Systeme:

- **1a: Mainframes/Terminals, dedizierte Software**
- **1b: Datenbanken, Office Anwendungen**

Phase 2.1 (1985+): Dezentralisierung mit dedizierten Netzen:

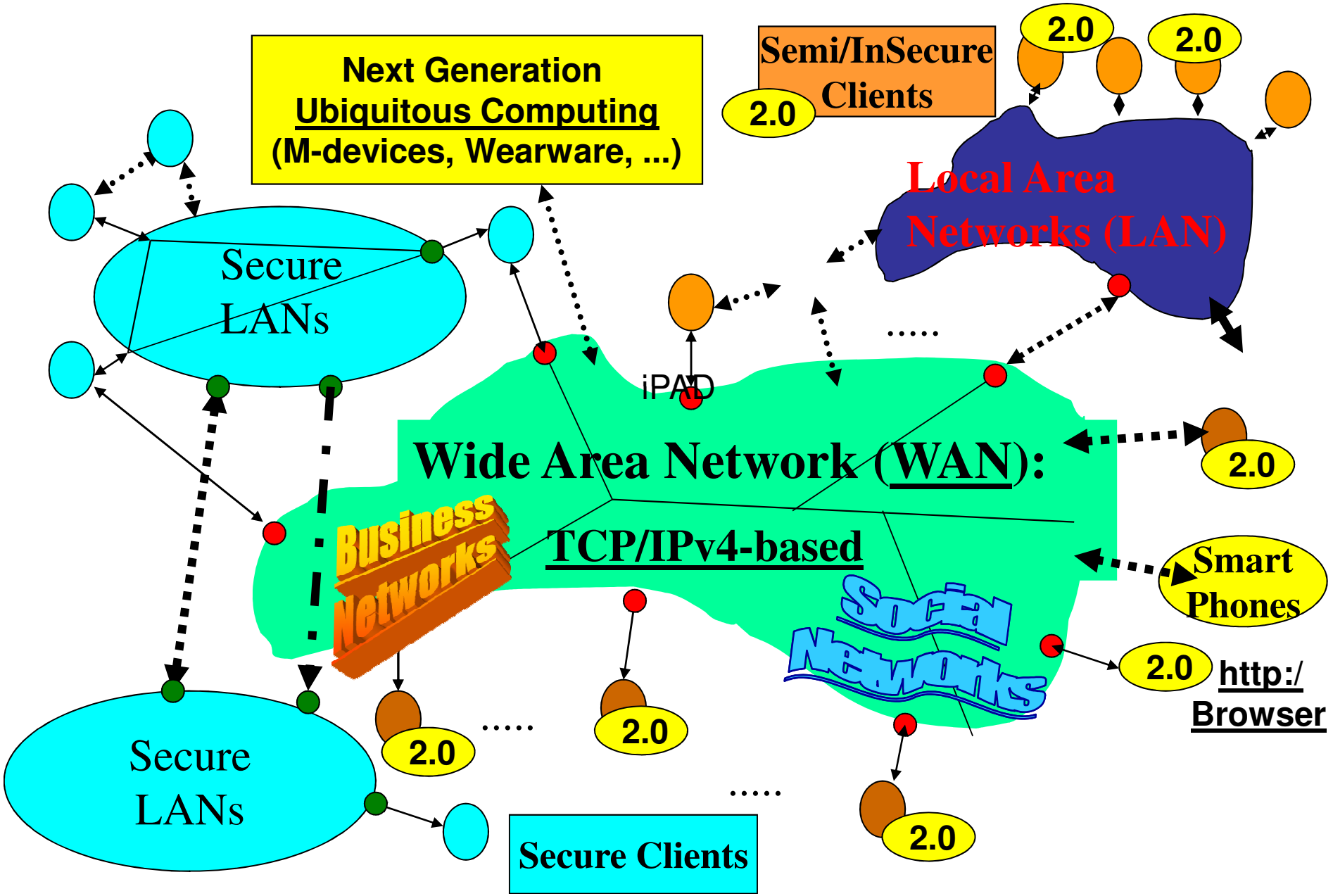
- **2a: Personal Computer, Mainframes und LANs**
- **2b: Client-Server Architekturen, Enterprise Anwendungen**

Phase 2.2(2000+): Globalisierung mittels Internet & Web 2.0:

- **2c: Lokale & globale Kommunikation über IP-Protokoll**
- **2d: Einsatz des World Wide Web (html, htt-Protokoll)**
- **2e: Business Intelligence, Kommunikation & Motivation (Social Media)**

1.6: „Information Society“ and Web 2.0:

2011: ~1M Server, ~1.5 G Klienten



1.7 Zur Entwicklung des IKT-Einsatzes in Unternehmen: Von Mainframes zu Enterprise 3.0:

Zur Einordnung: Ein kurzer Abriss des Zeitablaufes

Phase 1 (1960+): Zentralisierte IT-Systeme:

- **1a: Mainframes/Terminals, dedizierte Software**
- **1b: Datenbanken, Office Anwendungen**

Phase 2.1 (1985+): Dezentralisierung mit dedizierten Netzen:

- **2a: Personal Computer, Mainframes und LANs**
- **2b: Client-Server Architekturen, Enterprise Anwendungen**

Phase 2.2 (2000+): Globalisierung mittels Internet & Web 2.0:

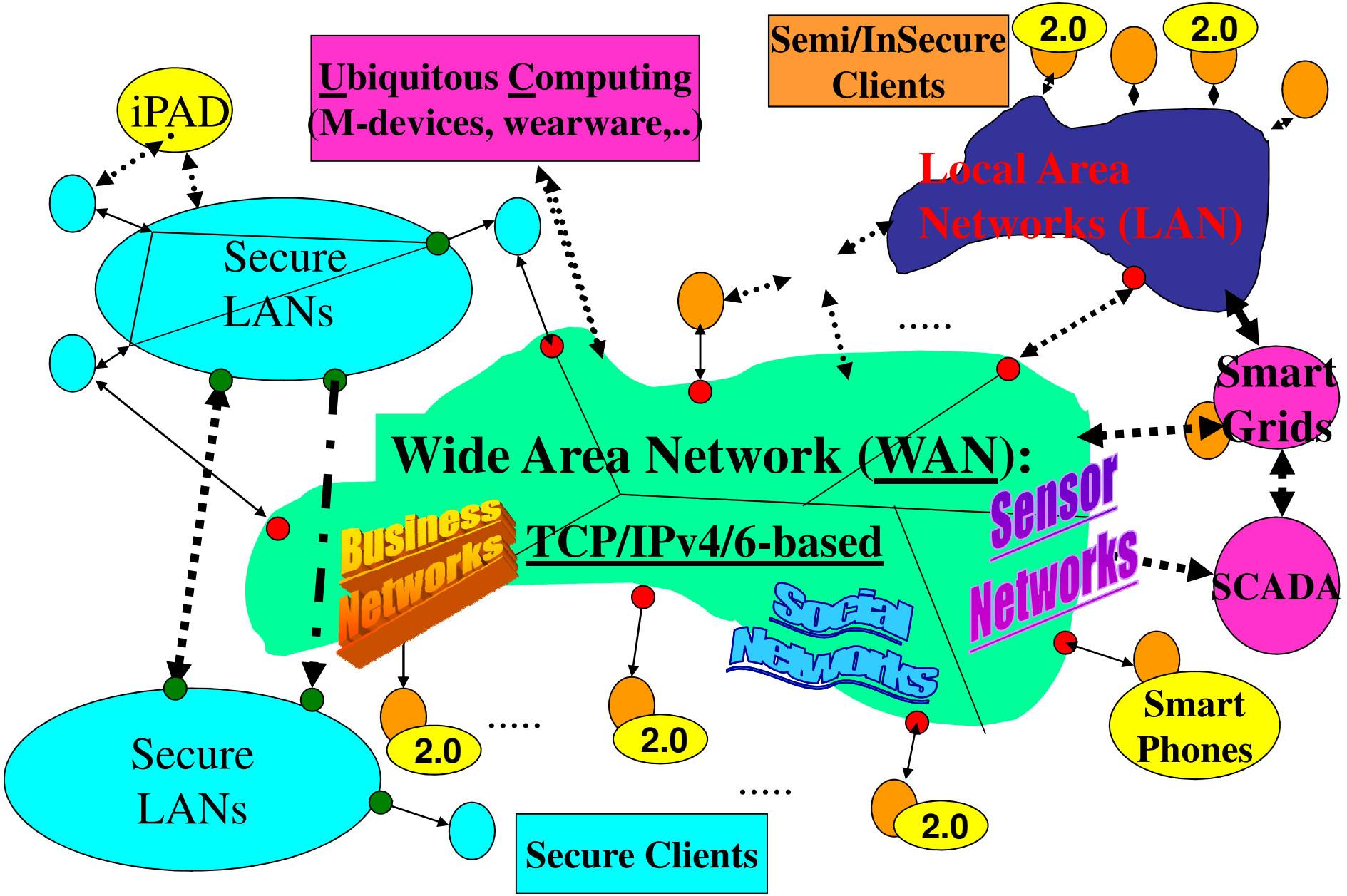
- **2c: Lokale & globale Kommunikation über IP-Protokoll**
- **2d: Einsatz des World Wide Web (html, htt-Protokoll)**
- **2e: Business Intelligence, Kommunikation & Motivation (Social Media)**

Phase 2.3 (2010+): RealTime-Verarbeitung: Enterprise 3.0

- **2f: Angriffe auf ungesicherte IKT-Systeme (IP v4)**
  - **→ Angriffe auf SCADA-Anlagen, z.B. Stuxnet**
- **2g: Einsatz von IPv6,**
  - **Geschützte verbundene IKT-Produktionssteuerungen**

1.8 „Information Society“and „Web 3.0“:

2015: ~1M Server, ~5G Klienten, >1T Sensors(“Smart Grids“)



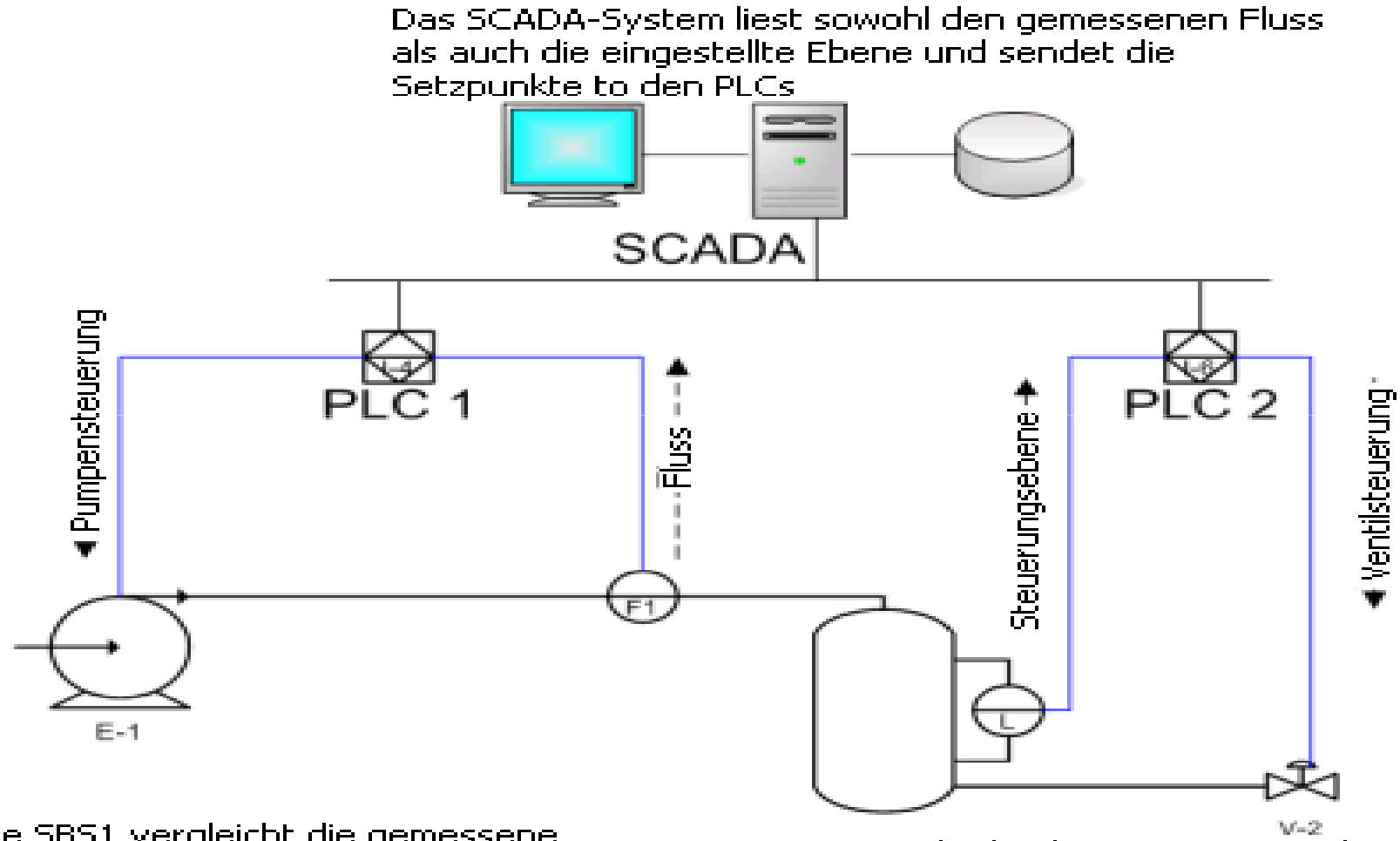
2.1 Begriffsbestimmung SCADA:

Quelle Wikipedia:

SCADA: Supervisory Control and Data Acquisition:

„Unter **Überwachung, Steuerung, Datenerfassung** (ÜSE), oft englisch **Supervisory Control and Data Acquisition** (SCADA), wird das Konzept zur Überwachung und Steuerung technischer Prozesse verstanden.“

2.2 Beispiel SCADA (Wikipedia):



Die SBS1 vergleicht die gemessene Durchflussgeschwindigkeit zu Sollwert und steuert die Pumpe so, dass die sie dem Sollwert entspricht.

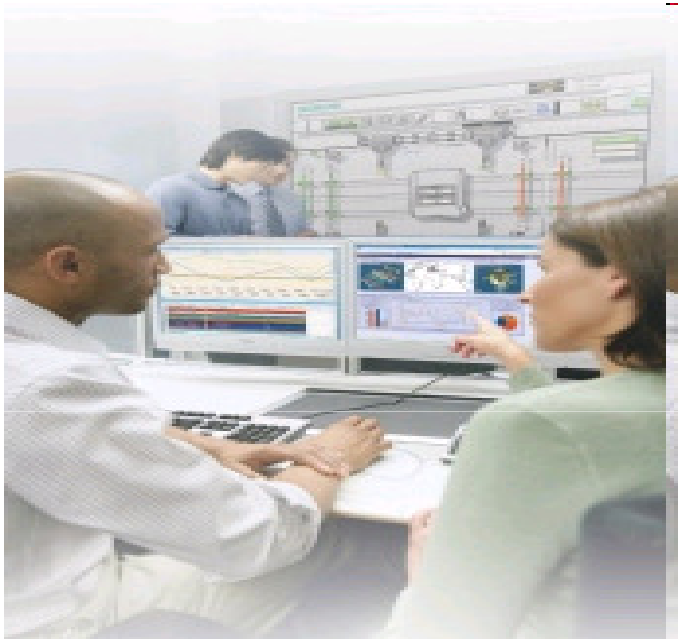
SBS2 vergleicht die gemessenen Ebenen zu dem Sollwert und steuert den Durchfluss durch das Ventil, sodass er dem Sollwert entspricht.

2.3a SCADA Beispiel: Siemens SIMATIC WinCC

Quelle: http://www.automation.siemens.com/

„Prozessvisualisierung mit Plant Intelligence

Unsere SCADA-Software bietet höchste Funktionalität und eine benutzerfreundliche Bedienoberfläche. Mit dem projektier- und skalierbaren System profitieren Sie von absoluter Offenheit zu Bürowelt und Produktion – z. B. via integrierter Prozessdatenbank und durch Plant Intelligence für mehr Transparenz in der Produktion. Zahlreiche Optionen und Add-ons ergänzen und erweitern den Leistungsumfang“



„Branchenlösungen mit SIMATIC WinCC

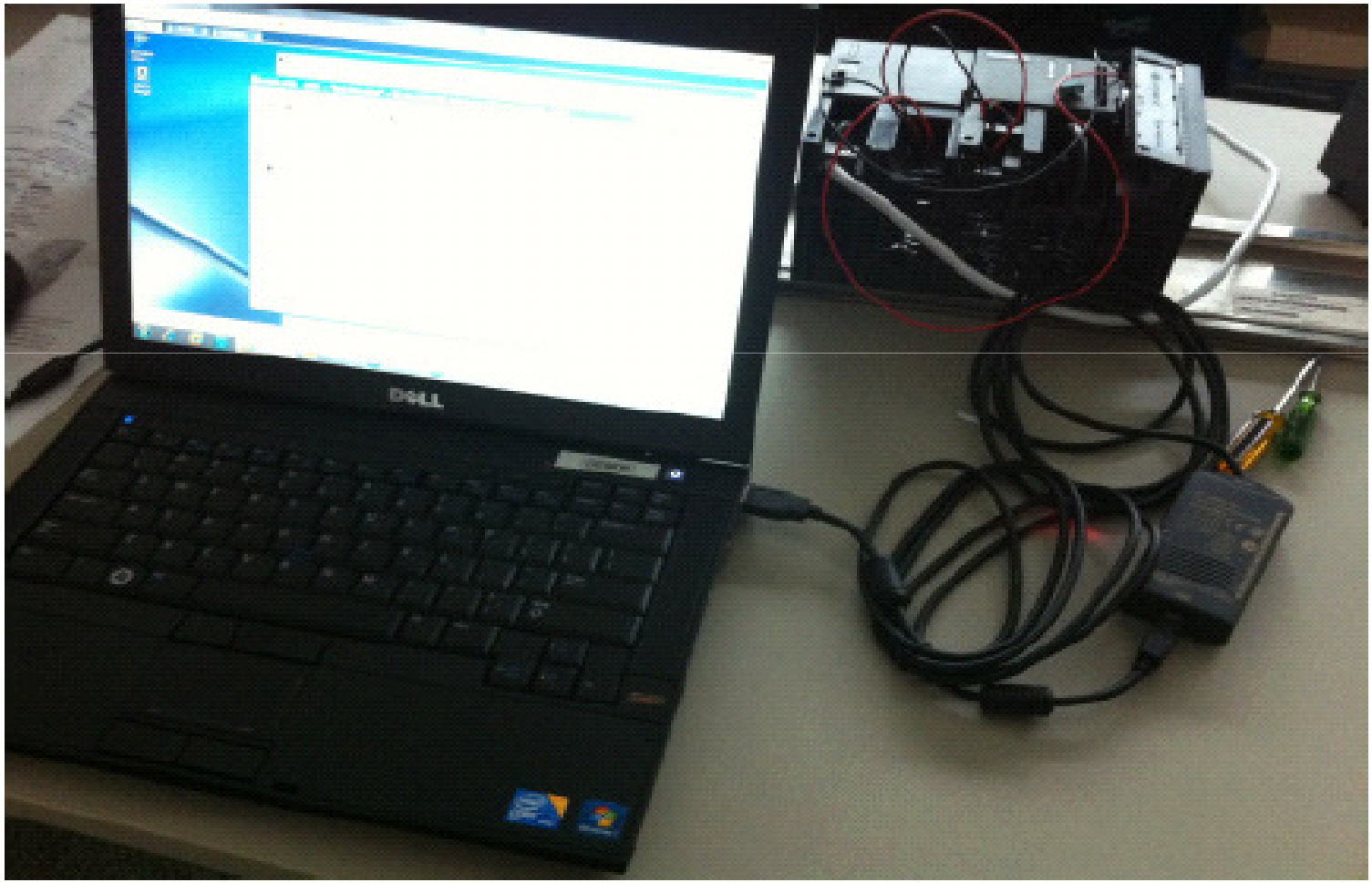
Erfahren Sie, wie Sie aus dem branchenneutralen SCADA-System WinCC mit den richtigen Optionen und Add-ons eine lmaßgeschneiderte Branchenlösung erstellen können.“

Anmerkung: Kopie (sic!) der SIMATIC Webseiten (1/2).

2.3b Siemens Simatic PLC 101

Figure 16

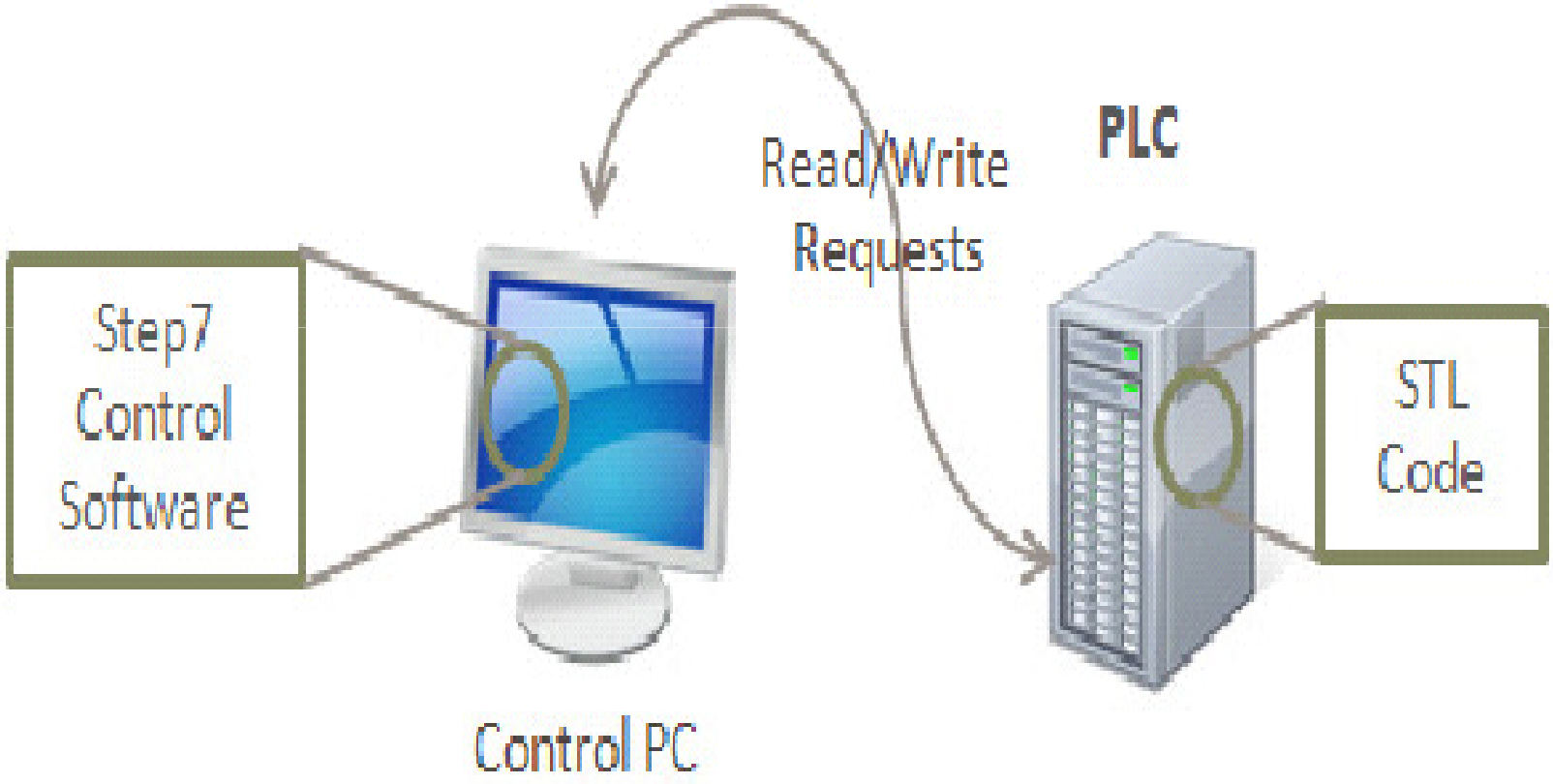
Test equipment



2.3c Siemens Simatic PLC and WinCC/Step 7

Figure 15

PLC and Step7



3.1a CyberAttacks 1992-2006 on SCADA Systems #1

Source: Filip Maertens - Cyber threats to critical infrastructures :

1992 -- Chevron -- Emergency system sabotaged by disgruntled employee in over 22 states

1997 -- Worchester Airport -- External hacker shut down air/ground traffic communication system for 6 hours

1998 -- Gazprom -- Foreign hackers seize control of main EU gas pipelines using trojan horse attacks

2000 -- Queensland, Australia -- Disgruntled employee hacks into sewage system and releases over a million liters of raw sewage into the coastal waters

2002 -- Venezuela Port -- Hackers disable PLC components during a national unrest and general workers strike, disabled the country's main port

3.1b CyberAttacks 1992-2006 on SCADA Systems #2

2003 -- U.S East Coast blackout -- A worm did not cause the blackout, yet the Blaster worm did significantly infect all systems that were related to the large scale power blackout

2003 -- Ohio Davis-Besse Nuclear Plant -- Plant safety monitoring system was shut down by the Slammer worm for over five hours

2003 -- Israel Electric Corporation -- Iran originating cyber attacks penetrate IEC, but fail to shut down the power grid using DoS attacks

2005 -- Daimler Chrysler -- 13 U.S manufacturing plants were shut down due to multiple internet worm infections (Zotob, RBot, IRCBot)

2005 -- International Energy Company -- Malware infected HMI system disabled the emergency stop of equipment under heavy weather conditions

3.1c CyberAttacks 1992-2006 on SCADA Systems #3

2006 -- Middle East Sea Port -- Intrusion test gone wrong. ARP spoofing attacks shut down port signaling system

2006 -- International Petrochemical Company -- Extremist propaganda was found together with text files containing usernames & passwords of control systems

……..

2010: Worldwide: „Virus“ Stuxnet infects 10.000s of Siemens WinCC/PCS 7 systems, including controllers for uranium centrifuges

3.1d About the QLD/Australia attack in 2000:

"*That was the case in Australia in April 2000. Vitek Boden, a former contractor, took control of the SCADA system controlling the sewage and water treatment system at Queensland's Maroochy Shire.* ***Using a wireless connection and a stolen computer, Boden released millions of gallons of raw sewage and sludge into creeks, parks and a nearby hotel.*** *He later went to jail for two years. Not surprisingly, U.S. companies are hesitant to talk about the security of their SCADA networks for fear they may give clues to hackers. But security consultants say problems with them are widespread. Allor's company, for instance, regularly does audits of SCADA systems at major installations such as power plants, oil refineries and water treatment systems.*

Almost invariably, Allor said, the ***companies claim their SCADA systems are secure and not connected to the Internet****. And almost invariably, he said, ISS consultants find a wireless connection that company officials didn't know about or other open doors for hackers. Realizing the growing threat, the federal government two years ago directed its Idaho National Laboratory to focus on SCADA security. The lab created the nation's first "test bed" for SCADA networks and began offering voluntary audits for companies.*"

(Anmerkung: **Hervorhebung** des Referenten)

4.1 STUXNET (2010) Goals:

Source: Symantec „W32.Stuxnet Dossier“, September 2010

Executive Summary:

Stuxnet is a threat targeting a specific industrial control system (*) likely in Iran(*), such as a gas pipeline or power plant.

The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLC)

(PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries.

Stuxnet was discovered in July 2010, but is confirmed to have existed at least one year prior and likely even before.

Comments: (*) SIMATIC WinCC, speculation/counter evidence,

(**) First STUXNET known since November 2008!

4.2 STUXNET (2010) Propagation:

…. Stuxnet contains many features such as:

Self-replicates through removable drives **(USB!)** exploiting a vulnerability allowing auto-execution.

Spreads in a LAN through a vulnerability in the **Windows Print Spooler (***)**.

Copies and executes itself on remote computers through network shares.

Copies and executes itself on remote computers running a WinCC database server loaded.

Comment: (***) **Microsoft Vulnerabilities**

4.3 STUXNET (2010) Exploits MS Vulnerabilities:

Updates itself through a peer-to-peer mechanism within a LAN.

Exploits a total of 4 unpatched Microsoft vulnerabilities, 2 of which are **previously mentioned vulnerabilities for self-replication** and the other two are **escalation of privilege vulnerabilities** that have yet to be disclosed.

Contacts a command and control server that allows the hacker to download and execute code, including updated versions.

- Contains a Windows rootkit that hide its binaries.
- Attempts to bypass security products.
- Fingerprints a specific industrial control system and modifies code on the Siemens PLCs to potentially sabotage the system.
- Hides modified code on PLCs, essentially a rootkit for PLCs.

4.4 STUXNET (2010) Timeline (#1/2)

Timeline W32.Stuxnet Timeline (#1)

→ November 20, 2008 Trojan.Zlob variant found to be using the LNK vulnerability only later identified in Stuxnet.

→ April, 2009 Security magazine Hakin9 releases details of a remote code execution vulnerability in Printer Spooler service (later MS10-061).

→ June, 2009 Earliest Stuxnet sample seen (no exploit MS10-046/ no signed driver files).

→ January 25, 2010 Stuxnet driver signed with a valid certificate belonging to Realtek Semiconductor Corps.

→ March, 2010 First Stuxnet variant to exploit MS10-046.

→ June 17, 2010 Virusblokada reports W32.Stuxnet (named RootkitTmphider). Reports that it's using a vulnerability in the processing of shortcuts/.lnk files in order to propagate (later identified as MS10-046).

→ July 13, 2010 Symantec adds detection as W32.Temphid (previously detected as Trojan Horse).

→ July 16, 2010 Microsoft issues Security Advisory for "Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)" that covers the vulnerability in processing shortcuts/.lnk files.

Verisign revokes Realtek Semiconductor Corps certificate.

4.5 STUXNET (2010) Timeline (#2/2)

Timeline W32.Stuxnet Timeline cont. (#2)

→ July 17, 2010 Eset identifies a new Stuxnet driver, this time signed with a certificate from JMicron Technology Corp.

→ July 19, 2010 Siemens report that they are investigating reports of malware infecting Siemens WinCC SCADA systems.

Symantec renames detection to W32.Stuxnet.

→ July 20, 2010 Symantec monitors the Stuxnet Command and Control traffic.

→ July 22, 2010 Verisign revokes the JMicron Technology Corps certificate.

→ August 2, 2010 Microsoft issues MS10-046, which patches the Windows Shell shortcut vulnerability.

→ August 6, 2010 Symantec reports how Stuxnet can inject and hide code on a PLC affecting industrial control systems.

→ September 14, 2010 Microsoft releases MS10-061 to patch the Printer Spooler Vulnerability identified by Symantec in August.

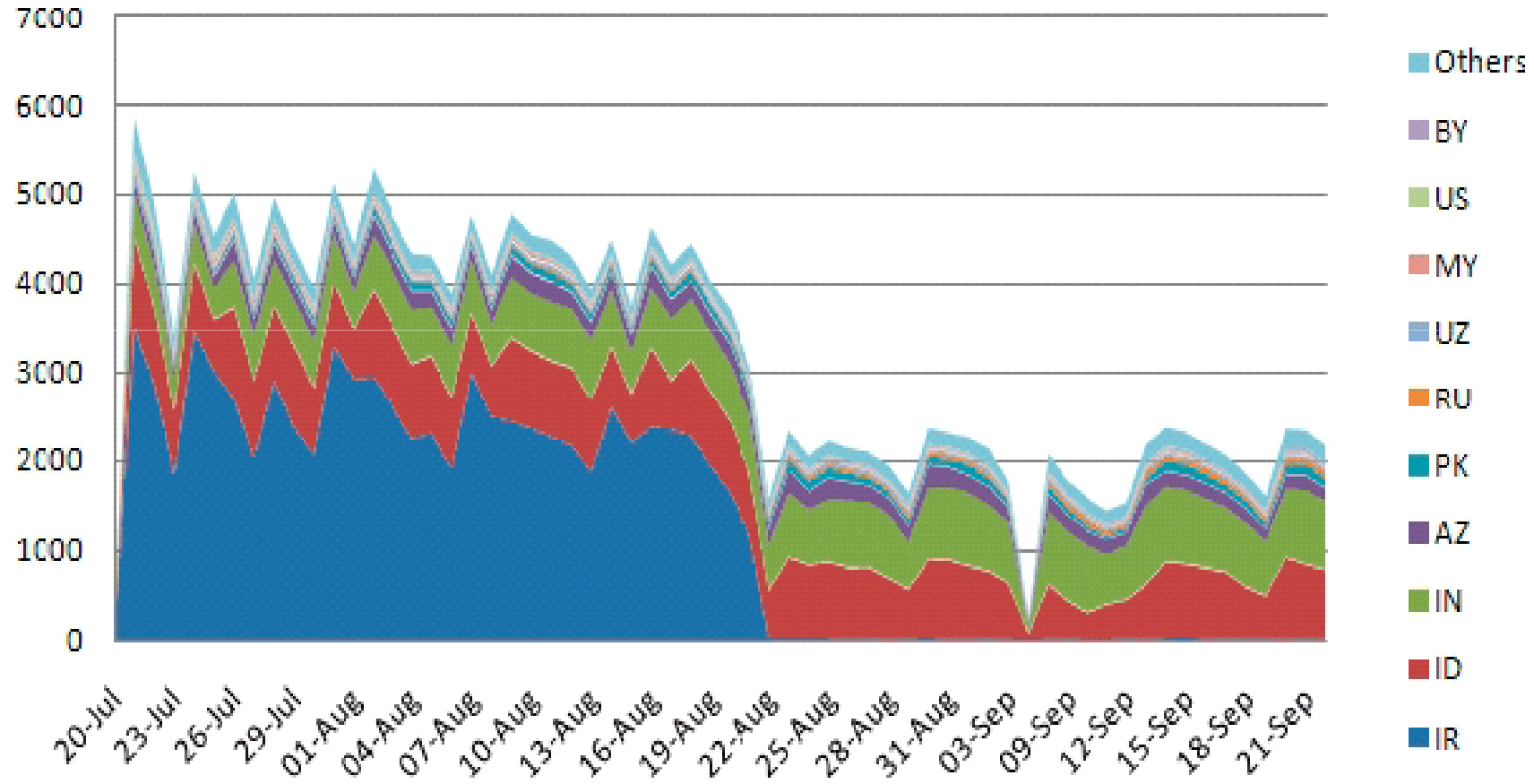
→ Microsoft report two other privilege escalation vulnerabilities identified by Symantec in August.

→ September 30, 2010 Symantec presents at Virus Bulletin and releases comprehensive analysis of Stuxnet.

4.6 Stuxnet (2010): Infection by Country

Figure 5

Rate of Stuxnet infection of new IPs by Country



Internetabkürzungen: IR=Iran, ID=Indonesien, IN=Indien, AZ=Azerbeidshan, PK=Pakistan, RU=Russland, ZU=Uzbekistan, MY=Malaysia, US=USA, BY=Belarus

4.7 STUXNET (2010) functions:

4.7a Stuxnet Infection Routine flow

4.7b Stuxnet Command and Control flow

4.7c Stuxnet Downloading latest Version

Remark: folios discussed in presentation, but not for distribution, following aVTC (Uni-Hamburg) ethical principle „Never distribute essential details of malicious code or malicious code in an executable form!“

Remark: aVTC = antiVirus Test Center, University of Hamburg

5.1 STUXNET zwischen Erkenntnis und Spekulation

Stand der „Berichterstattung“ (Spekulation ☺):

New York Times (15.1.2011): „Israeli Test on Worm Called Crucial in Iran Nuclear Delay“
Autoren: W.J.Broad, J.Markoff, D.E.Sanger

Forbes (17.1.2011): „The New York Times Fails To Deliver Stuxnet’s Creators“
Autor: J. Carr

Spiegel Online (18.1.2011): „Stuxnet: Angst vor einem zweiten Tschernobyl“
Autor: J.Patalong

These: die Israelis waren es, mit Hilfe der USA (dort Analyse der Siemens-Technologie)

Gegenrede: es gibt keinerlei Beweise, wer die Autoren waren!

Vermutung: „Stuxnet wirkt… Manche Experten befürchten den GAU, wenn infizierte Anlagen dennoch ans Netz gehen, und warnen vor mög-lichen Nachahmer-Attacken“

6. Weshalb sind Cyber-Angriffe möglich?

These: Heutige I&K-Techniken sind unsicher

Weil heutige I&K-Techniken waren originär für wissenschaftliche Zwecke entwickelt worden (vor allem: IP und WWW), bei denen Sicherheitsforderungen unwichtig waren!

Daher weisen heutige I&K-Techniken in Konzeption, Realisierung sowie in Einsatz und Nutzung erhebliche Mängel auf, was zu erheblichen Risiken führt. Dies verleitet viele Nutzer zu riskanten Handlungsweisen („dont care“, „es wird schon nichts passieren“)

6.1 Die Realität: Risiken/Überblick (unvollständig!)

- **Fehlfunktionen: vom Versagen bis zu schweren Unfällen**
- **Spamming: Überschwemmung mit nutzloser Email**
- **Hacking**: Angriffe auf Unternehmen+Staat
- **Malware: Viren, Würmer, Trojanische Pferde, ... Bösartige Software in Hand-Held Devices (Smartphones, iPAD, …)**
- **Internet ist Fundgrube für Maliziöse Software**
- **Miserable Software-Qualität** ermöglicht Mißbrauch
- **Schnüffelprogramme** ermöglichen **Abhörung**
- **Adreßfälschung** einfach zu realisieren
- **Phishing**: **Irreführende Emails leiten zu kriminellen Websites**
- **Pharming: verdeckte Form von Phishing**
- **Datenraub, Datenfälschung** (data hijacking) einfach
- **Massive automatische Denial-of-Service Angriffe**
- **Business InfoWar: Datenkriege zwischen Unternehmen**
- **Organisierte Kriminalität mithilfe von I&K-Techniken**

6.2 Schutzmaßnahmen

6.2.1 Cyber Defence (D): „Die Wacht am Rhein“

6.2.2 (Gegen-)Angriff (Offence) ist die beste Verteidigung:
„Persona Management System“,
Angriffe der „sock puppets“

6.2.3 Indien (Cyber Offence): Hacker als Hilfstruppen

6.2.1.1 Cyber Verteidigung (D): „Die Wacht am Rhein“

Quelle: SPIEGEL Online 27.12.2010:

Computer Spionage:
Bundesregierung plant Cyber-Abwehrzentrum

Behördencomputer sind immer heftigeren Angriffen aus den Internet ausgesetzt. Dem Bundesinnenministerium zufolge gehen die meisten davon von China aus. Jetzt soll ein spezielles Abwehrzentrum die Angreifer in Schach halten - und vor allem wichtiges Wissen schützen.

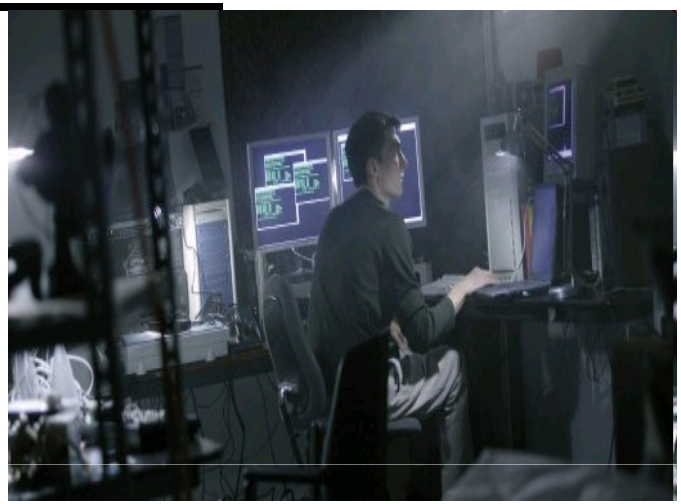
6.2.1.2 Cyber Verteidigung (D): „Die Wacht am Rhein“

Computer in Bundesministerien und anderen Behörden werden immer öfter **Opfer von Cyber-Attacken**. "Es gibt eine deutliche Zunahme dieser sogenannten elektronischen Angriffe auf deutsche Regierungs- und Behördennetze", berichtete der Sprecher des Bundesinnenministeriums, Stefan Paris, am Montag in Berlin. **Allein zwischen Januar und September dieses Jahres wurden 1600 derartige Angriffe registriert**. Die meisten davon seien von China ausgegangen. 2011 plant die Regierung deshalb, ein **nationales Cyber-Abwehrzentrum** einzurichten.

Noch **2009** habe die Zahl der festgestellten elektronischen Attacken auf Behördenrechner **im gesamten Jahr bei rund 900 gelegen**, erklärte Paris. Eine Sprecherin des Bundesamts für Verfassungsschutz sagte gegenüber der WAZ-Gruppe, ihre Behörde beobachte diese Entwicklung bereits seit 2005. Zudem gebe es eine **hohe Dunkelziffer**.

6.2.1.3 Cyber Verteidigung (D): „Die Wacht am Rhein“

Quelle: SPIEGEL Online 12.2.2011



Koalitionsstreit:
FDP kritisiert Pläne für Cyber-Abwehrzentrum

Im April soll das "Nationale Cyber-Abwehrzentrum" in Bonn eröffnet werden - jetzt gibt es nach Informationen des SPIEGEL Streit in der Koalition über die staatliche Hacker-Abwehr. Die FDP befürchtet eine unzulässige "Vermischung polizeilicher und nachrichtendienstlicher Tätigkeiten".

Anmerkung: inzwischen hat das Kabinett die Einrichtung des NCAZ beschlossen. Es soll beim BSI eingerichtet werden.

6.2.2.1 Aktuelles: Cyber Warrior (USA)

17. März 2011 SPIEGEL Online (*):
„US-Cyber-Krieg
über Facebook und Co.
Angriff der Sockenpuppen“

(*) Alle Zitate aus diesem Artikel

„Sock Puppets“ (Sockenpuppen) sind erfundene oder gestohlene Identitäten, mit Denen online Meinungen und (Des-)Informationen verbreitet werden können, etwa über Blogs, Forenkommentare oder Wikipedia usw.

„Schlachten werden auch über Facebook und Twitter geschlagen - das haben die Revolutionen Arabiens bewiesen. Cyber-Krieger im Pentagon haben nun Software bestellt, mit der sie Meinung im Netz manipulieren können - in Farsi, Arabisch, Urdu und Paschtu. In den USA selbst wäre das illegal.“

6.2.2.2 Aktuelles: CyberWarrior (USA)

(*) Washington - Das US-Militär sieht sich für einen Cyber-Krieg mangelhaft gerüstet. Die **Cyber-Abwehr** der Vereinigten Staaten sei derzeit **"sehr dünn",** warnte General Keith Alexander eben erst den US-Kongress. Alexander ist der **Chef des "Cyber Command"** im US-Verteidigungs-ministerium. Man habe derzeit "nicht die Kapazitäten, die wir brauchen, alles zu erreichen, was wir erreichen müssen", so der oberste Cyber-Krieger der USA. So könne man sich **"nicht erlauben, dass der Cyberspace ein Schutzraum ist, in dem echte und potentielle Gegner ihre Truppen und Fähigkeiten gegen uns und unsere Verbündeten in Stellung bringen können".** Es handele sich dabei **"nicht um eine hypothetische Gefahr",** so der General.

6.2.2.3 Aktuelles: CyberWarrior (USA)

23.2.2011 SPIEGEL Online (*):

über eine Ausschreibung der US Airforce (FBO.gov):

„Die Air Force sucht einen Zulieferer, der eine sog. "Persona Management Software" schreibt. Das System soll es jedem Anwender ermöglichen, mit bis zu zehn Tarnidentitäten im Netz unterwegs zu sein. Der Anspruch der Auftraggeber an die Tarnidentitäten: "Es muss möglich sein, eine solche Person in jeder Region der Welt zu verorten." Die im Netz platzierten Details sollten auch für "erfahrene Gegner" nicht als Fälschung zu erkennen sein.

„Im Klartext: Da bestellt sich das Militär ein Management-Werkzeug zum Anlegen, Verwalten und Nutzen digitaler Legenden für Einsatzkräfte. Zu welchem Zweck ist unklar. Denkbar ist einiges: Verbreiten von Propaganda, Aushorchen von Quellen, Schutz der Tarn-Identitäten exponierter Mitarbeiter.“

6.2.2.4 Aktuelles: CyberWarrior (USA)

Dazu nennt SPIEGEL Online als Bewerber:

„Rechner infiltrieren, Nutzer belauschen, Tarnidentitäten im Web pflegen: Die US-Sicherheitsfirma HBGary liefert Abwehr- und Spionage-Software. Zu den Kunden gehören auch die Sicherheitsbehörden der USA. Nun geben entwendete Firmen-E-Mails einen Einblick in das Geschäft mit dem digitalen Krieg."

Aus dem Portfolio von HBGary für Angriffs-Software:

- **Die Schnüffelprogramme sollen Tastatureingaben protokollieren und … das System nach Dateien mit bestimmten Schlagworten im Inhalt durchsuchen, diese Daten Huckepack mit gewöhnlichem Datenverkehr beim Webbrowsen übertragen. (Anmerkung: Lizenzgebühr: 6,000 US$)**
- **Gängige Anti-Rootkit-Schutzprogramme sollen die Anwendungen nicht bemerken.**
- **Die Schadsoftware soll von Firewall-Software ungehindert mit der Steuereinheit über Internet-Traffic kommunizieren, den Datenverkehr nach außen in anderem Netzwerk-Traffic verbergen.**
- **Die Schnüffelprogramme sollen über verschiedene Wege einschleusbar sein - Web-Seiten, zu öffnende Dateien, E-Mail, übertragene Datenpakete.**

6.2.2.5 Aktuelles: CyberWarrior (USA)

(+) **Fachliche Beurteilung:** Der Informatiker Thorsten Holz (Professor für Embedded Malware, Ruhr-Uni Bochum) urteilt: "Die Projektvorschläge von HBGary Federal, die ich gelesen habe, klingen fachlich korrekt. Die Autoren diskutieren und wägen verschiedene Ansätze ab, die alle sinnvoll sind."

Das Schicksal der Firma HBGary:

Nachdem HBGary die Identitäten der Hacker-Gruppe „Anonymous“ – die u. a. als Unterstützer von Wikileaks auch Angriffe auf US-Unternehmen Payback und VISA Durchgeführt haben sollen – im Internet veröffentlichen Wollten, wurden zahlreiche Emails von HBGary durch „Anonymous“ veröffentlicht. Daraufhin trat zunächst der CEO zurück.

(+) Quelle: c´t 6/2011: „Ausgelacht: Anonymous kompromittiert US-Sicherheitsfirma“

6.2.2.6 Aktuelles: CyberWarrior (USA)

Den Auftrag der US Air Force, für 2,78 Mio US$ diese „Persona Management Software“ zu erstellen, erhielt die kalifornische Firma "Ntrepid" (intrepid = furchtlos).

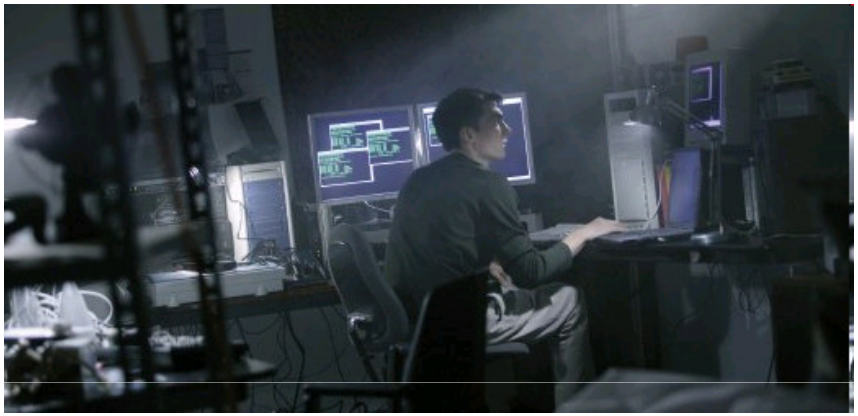
Der "Guardian" zitiert einen Sprecher des US-Oberkommandos Centcom: "Die Technologie ermöglicht geheime Blogging-Aktivitäten auf fremdsprachigen Websites, um Centcom in die Lage zu versetzen, der Propaganda von gewalttätigen Extremisten und Feinden von außerhalb der USA zu begegnen." Die Sockenpuppen des US-Militärs sollen allerdings nicht englisch schreiben dürfen, so der Sprecher weiter, denn es würde gegen das Gesetz verstoßen "sich an ein US-Publikum zu wenden". Die gefälschten Identitäten sollen stattdessen Netznachrichten auf Arabisch, Farsi, Urdu und Paschtu absetzen.

6.2.3.1 Indien: Hacker als Hilfstruppen

15. März 2011 SPIEGEL Online (*):

„Cyber War: Indien rekrutiert Hacker zur Selbstverteidigung“

(*) Alle Zitate aus diesem Artikel



Bericht von einer „MalCon“ in Mumbai: "Wir brauchen die Unterstützung der indischen Hackergemeinde, um den Cyberspace unseres Landes zu verteidigen", ruft ein **Regierungsvertreter** den Anwesenden zu. Obwohl der Beamte, der als enger Berater des indischen Regierungschefs gilt, in der Öffentlichkeit spricht, möchte er seinen Namen nicht in der ausländischen Presse lesen. **"Es gibt viele talentierte Hacker in Indien, wir müssen sie finden und ihre Fähigkeiten ausmachen. Daher soll Malcon uns als Kommunikationsplattform dienen",** so der Politiker weiter.

6.2.3.2 Indien: Hacker als Hilfstruppen

Ein Frühwarnsystem wie für Tsunamis

Rajshekhar Murthy, Organisator der Veranstaltung, legt Wert darauf, dass die Plattform **kein Treffpunkt für Kriminelle** sein soll. Wenngleich es schwer fallen dürfte, hier eine klare Linie zu ziehen. **"Die gleiche Technik, die zum Klauen von Kreditkarteninformationen dient, kann auch beim Verteidigen der digitalen Infrastruktur eines Landes helfen",** sagt Murphy SPIEGEL ONLINE. "Die gleichen Hacker, die geschickt sind beim Programmieren solcher Software oder beim Umgehen von Schutzmechanismen, können ihre Fähigkeiten auch in den Dienst ihres Heimatlandes stellen." Murthy schwebt ein Netzwerk vor, eine **Gemeinschaft aus wachsamen Hackern als Frühwarnsystem**.

Meldet ein Hacker Verdächtiges - der Regierungsvertreter vergleicht die übers Land verstreuten Sicherheitsexperten mit auf hoher See verteilten **Tsunami-Frühwarnsensoren** - werden die gelieferten Informationen auf **Stichhaltigkeit überprüft**. Von einer Überprüfung der Vergangenheit der beteiligten IT-Freaks ist im Umfeld der Malcon zwar nie die Rede. Kommt es jedoch zu einer Zusammenarbeit, dann wollen die Verantwortlichen den Hackern **Verhaltensregeln** ans Herz legen: **Keine bösartige Malware mehr, kein Veröffentlichen von Schwachstellen im Netz, ohne den betroffenen Hersteller zu informieren ("full disclosure").**

Danke für Ihre Aufmerksamkeit!

Noch Fragen, bitte?