
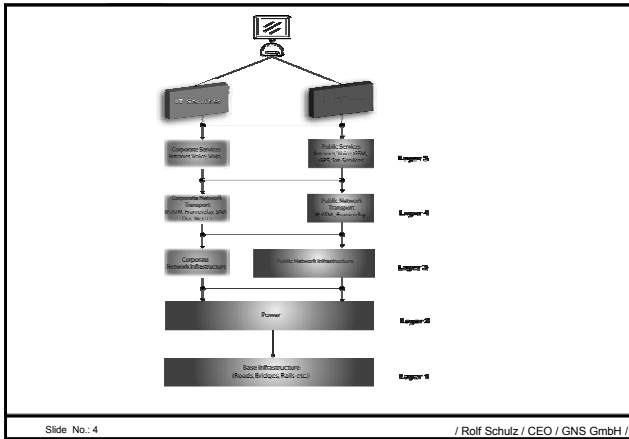


	Global Network Security GmbH
	CIP A Business View
Rolf Schulz CEO	

	Global Network Security GmbH
Definition	
<p>✓ critical infrastructure:</p> <ul style="list-style-type: none"> ➤ 1. Elements of a <u>system</u> that are so vital that disabling any of them would incapacitate the entire system. ➤ 2. [In <u>security</u>,] those physical and <u>cyber</u>-based systems essential to the minimum <u>operations</u> of the economy and government. [INFOSEC-99] 	
Slide No.: 2	/ Rolf Schulz / CEO / GNS GmbH /

	Global Network Security GmbH
<h1>The Battlefield</h1>	
Slide No.: 3	/ Rolf Schulz / CEO / GNS GmbH /



Global Network Security GmbH	
	Base infrastructure
<p>✓ Vulnerabilities</p> <ul style="list-style-type: none"> ➢ Only major incidents, like <ul style="list-style-type: none"> ▪ Dam failure <ul style="list-style-type: none"> • environmental causes • engineering causes ▪ Natural disaster <ul style="list-style-type: none"> • Earthquakes <ul style="list-style-type: none"> » Japan or West Coast USA • flood disaster • storms ▪ Sabotage ▪ Terrorism - large scale attacks <ul style="list-style-type: none"> • ABC attacks ▪ War 	
Slide No.: 5 / Rolf Schulz / CEO / GNS GmbH /	

Global Network Security GmbH	
	Electrical Power Infrastructure
<p>✓ Vulnerabilities</p> <ul style="list-style-type: none"> ➢ Natural disaster <ul style="list-style-type: none"> ▪ same as to base infrastructure ➢ Sabotage ➢ Engineering causes ➢ Construction Work ➢ External, IT based attacks against control software (even via Internet) <ul style="list-style-type: none"> ▪ COTS – commercial off the shelf software ➢ Terrorism - medium to small scaled attacks ➢ WAR 	
Slide No.: 6 / Rolf Schulz / CEO / GNS GmbH /	

Network Infrastructure

- ✓ Vulnerabilities
 - Natural disaster
 - same as to base infrastructure
 - Construction Work !!!!
 - 50% of Frankfurt City Net down due to a digger
 - Sabotage
 - 1999, the glass fiber cables of Lufthansa were cut by a unknown person.
 - Terrorism - medium to small scaled attacks
 - War

Generell Infrastructure Risk

- ✓ Who is the real owner of the infrastructure
 - More and more Infrastructure is sold to foreign companies
 - Glass fiber
 - Power lines
 - Telecommunication lines
 - Water
- ✓ Reason : Savings
 - Lease-Back
- ✓ No control on Hard- and Software
- ✓ And in an emergency case ???
 - National impact ???

Transport Service Infrastructure

- ✓ Vulnerabilities
 - IT Layer 2-4 attacks
 - DoS, ARP-Spoofing, etc...
 - Maintenance & Administration
 - Broadcast Storm renders corporate network useless during main business hours
 - wrong Port configuration on a switch
 - Hardware Failure
 - Interception of Services

Global Network Security GmbH

Service Layer

✓ Vulnerabilities

- IT Layer 5-7 attacks
 - E.g. manipulation of data , attacks of e-commerce systems etc.
 - (Global) DNS attacks
 - Backdoors
 - hostile programmers
 - "official" backdoors
- Manipulation of Services

Slide No.: 10 / Rolf Schulz / CEO / GNS GmbH /

Global Network Security GmbH

And the Enemy ?

Slide No.: 11 / Rolf Schulz / CEO / GNS GmbH /

Global Network Security GmbH

Security – Quo vadis

Hacker	-- calculable and – mostly- predictable, prevention possible
Internal risk	-- hard to guess, best to cover with organizational measures
Cyber crime	-- prevention not really possible
InfoWar	-- no prevention without support from the government

Slide No.: 12 / Rolf Schulz / CEO / GNS GmbH /

The Hacker

✓ Hackers World ...

- Ordinary hacker
 - very active, sometimes annoying, sometimes helpful
- Hacker by chance
 - more than annoying, often dangerous – he does not know, what he's doing
- Politically motivated hacker
 - a worldwide problem – not to be ignored
- Professional hacker
 - works accurately, mostly invisibly, a mercenary
- Organized crime hacker
 - very dangerous, with company, high skilled

Internal Risks

✓ The employee

- A trusted person
- Lives from 8 to 5 – no private background visible
- Anonym to his superior
- (Mostly) no background checks possible
- Often popular to his comrades
- Knows the company
- Knows the assets
- Knows all vulnerabilities

✓ The perfect Risk 😊

Cybercrime

✓ Definition

- **Cyber Crime refers to all the activities done with criminal intent in cyberspace or using the medium of Internet. These could be either the criminal activities in the conventional sense or activities, newly evolved with the growth of the new medium.**
- Often combines „traditional“ crime with IT related crime (blended attack)
- Mostly controlled by the organized crime

✓ Motivation

- Enrichment
- Terrorism
- Revenge

	Global Network Security GmbH
	C4i
<p>✓ C4i means</p> <ul style="list-style-type: none"> ➤ Command & Control, Communications, Computers and Intelligence – or Information Warfare ➤ Military playground for IT related attacks ➤ Targets : <ul style="list-style-type: none"> ▪ infrastructure of a nation, society, community ▪ military infrastructure ➤ One goal is to destroy the critical infrastructure like energy, transport, communication, financial business, etc. by the use of IT related attacks. ➤ Examples are viruses, worms or DoS/DDoS attacks ➤ Another goal is to manipulate or destroy military structures like Command & Control or Communications ➤ Alongside the use of IT related attacks also weapons like EMPs or High Power Microwave (HPM) Systems will be part of the attack scenario 	
Slide No.: 16	/ Rolf Schulz / CEO / GNS GmbH /

	Global Network Security GmbH
<h1>Intelligence ?</h1>	
Slide No.: 17	/ Rolf Schulz / CEO / GNS GmbH /

	Global Network Security GmbH
	Who's the enemy ??
<p>✓ Know your enemy</p> <ul style="list-style-type: none"> ➤ Who is your enemy ? ➤ What are the attackers' goals ? ➤ How is his skill ? ➤ What are his weapons ? ➤ What is his motivation ? ➤ How is his internal communication organized ? ➤ What does he knows about you ???? 	
Slide No.: 18	/ Rolf Schulz / CEO / GNS GmbH /

Some definition's

- ✓ Intelligence
 - Provision of information about the enemy and his possibilities
- ✓ "Battlefield" Intelligence
 - Provision of information about the enemy during a battle – his resources, tactics etc.
 - Map out your own strategy
 - Works hand in hand with Intelligence (Well...)

The Reality...

- ✓ What do we know about an IT attack and the people behind it? And when do we have the information ?
 - Intelligence
 - negative (rumors, black hat talking, so called insider information, etc.)
 - Battlefield intelligence
 - minimum, but you cannot expect more
 - Defense strategy
 - uncoordinated
 - Efficiency
 - nonexistent

Lessons ...

Germany and the RAF

- ✓ The activities of the terrorist group „RAF“ (Rote Armee Fraktion) were crucial for the German banks to take measures in protecting their infrastructure
 - In the late 80's, after the assassination of Alfred Herrhausen (Speaker of the Board, Deutsche Bank), a van filled with explosives, was found close to the IT Center of a German bank. The explosion would have destroyed the whole building.

Germany and the RAF

- ✓ Several attacks against Financial Institutions in Germany between 1970 and 1990
 - Bomb attacks
 - Assassinations
 - Kidnappings
 - Extortions
 - Bank robbery
- ✓ And the reaction ?
 - High availability for all critical systems and networks
 - Contingency organization and exercises
 - Rules and regulations from financial associations and the Ministry of Finance (e.g. backup regulations, MaH – Minimum requirements Trade) etc.

Typical Infrastructure today

- ✓ Minimum of two IT centers (primary and backup)
- ✓ Redundant glass fiber rings with separate routing (city net)
- ✓ Minimum of two separate house connections for data and power
- ✓ Two separate power links
- ✓ Minimum of two separate risers for the backbone inside a building, armored tubes for the cables
- ✓ Emergency workplace
- ✓ Backup Locations
- ✓ Continuity center

Typical Infrastructure today

- ✓ Minimum of three access points for the national and international network
- ✓ Minimum of 3 Pop's from different carriers and on different locations
- ✓ Three redundant basis services like ATM, Gigabit Ethernet und Dark Fiber
- ✓ Emergency power generator system
- ✓ UPS for all systems in IT center

Examples

- ✓ Bank lost Branch in WFC on 9/11
 - No losses, only minor injuries
 - Bank was back to business 24h later via backup location in Rye / New York (20 miles)
- ✓ Flood disaster in Prag
 - All major carrier lost equipment
 - Lot's of outages in the town over several days
 - Business restarted 24h later via backup location

CIP

	Global Network Security GmbH
<small>Excerpt from : THE NATIONAL STRATEGY TO SECURE CYBERSPACE</small>	
<ul style="list-style-type: none"> ✓ ... In general, the private sector is best equipped and structured to respond to an evolving cyber threat ✓ ...Public-Private engagement is a key component to secure cyberspace ✓ ... A federal role in these and other cases is only justified when the benefits of intervention outweigh the associated costs. This standard is especially important in cases where there are viable private sector solutions for addressing any potential threat or vulnerability. 	
Slide No.: 28	/ Rolf Schulz / CEO / GNS GmbH /

	Global Network Security GmbH
Government's Role	
<ul style="list-style-type: none"> ✓ International Coordination <ul style="list-style-type: none"> ➢ International cooperation, political preparation ✓ National Coordination <ul style="list-style-type: none"> ➢ Single Points of contacts (Cyber Squat, Alerting Service, National CERT for Support for non Cert Constituencies) ✓ Attack assessment <ul style="list-style-type: none"> ➢ Classification of attacks ✓ Forensic / Analysis <ul style="list-style-type: none"> ➢ something like a National Forensic Center ➢ Research Activities ➢ Sponsoring of initiatives ➢ Support of Universities 	
Slide No.: 29	/ Rolf Schulz / CEO / GNS GmbH /

	Global Network Security GmbH
Government's Role	
<ul style="list-style-type: none"> ✓ National Alarming Service ✓ Intelligence <ul style="list-style-type: none"> ➢ Information is a crucial factor. The government has the resources for such a "cyber-intelligence-service" ✓ Research <ul style="list-style-type: none"> ➢ Support of Universities, Sponsoring (together with industry) ✓ Awareness Programs ✓ Exercises <ul style="list-style-type: none"> ➢ CERT Coordination ➢ contingency training 	
Slide No.: 30	/ Rolf Schulz / CEO / GNS GmbH /

The private industrie's role

- ✓ Technical (know how) and organizational support
 - Private Industry has the know how, the experience, and the key technology
- ✓ Information Exchange
 - Private industry could provide different kinds of information.
 - A good starter can be statistical information on attacks from network IDS systems
 - Awareness Training
- ✓ Research, Training and Education
- ✓ CERT Team
 - Contact to national and international Certs
 - Know How Pool

How can this work ?

- ✓ Establish communication
 - Make sure, to understand the different cultures between government and industry
 - Involve not only the upper management, talk to the experts and convince them
 - Show the benefit for all involved partners
 - Make sure to have an open communi-cation - don't classify everything
