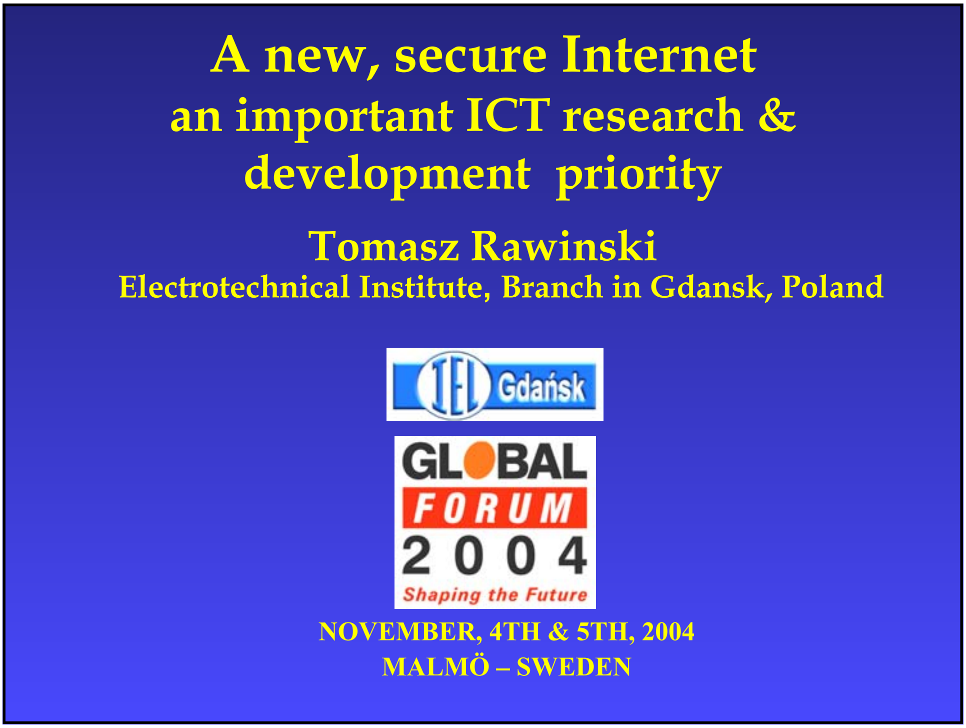
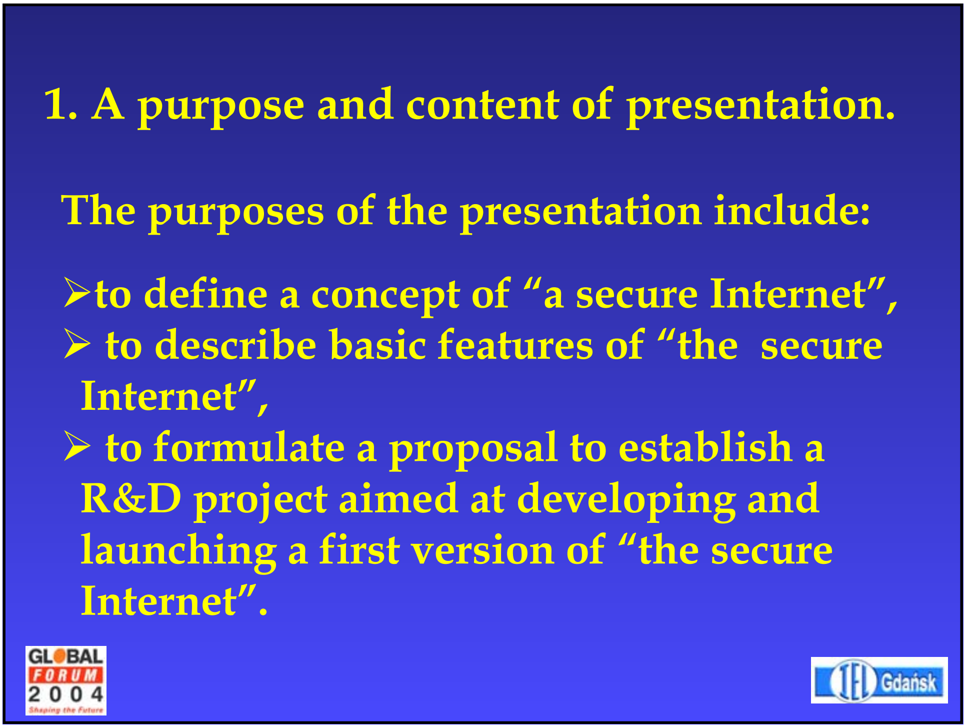


A new, secure Internet an important ICT research & development priority

Tomasz Rawinski
Electrotechnical Institute, Branch in Gdansk, Poland

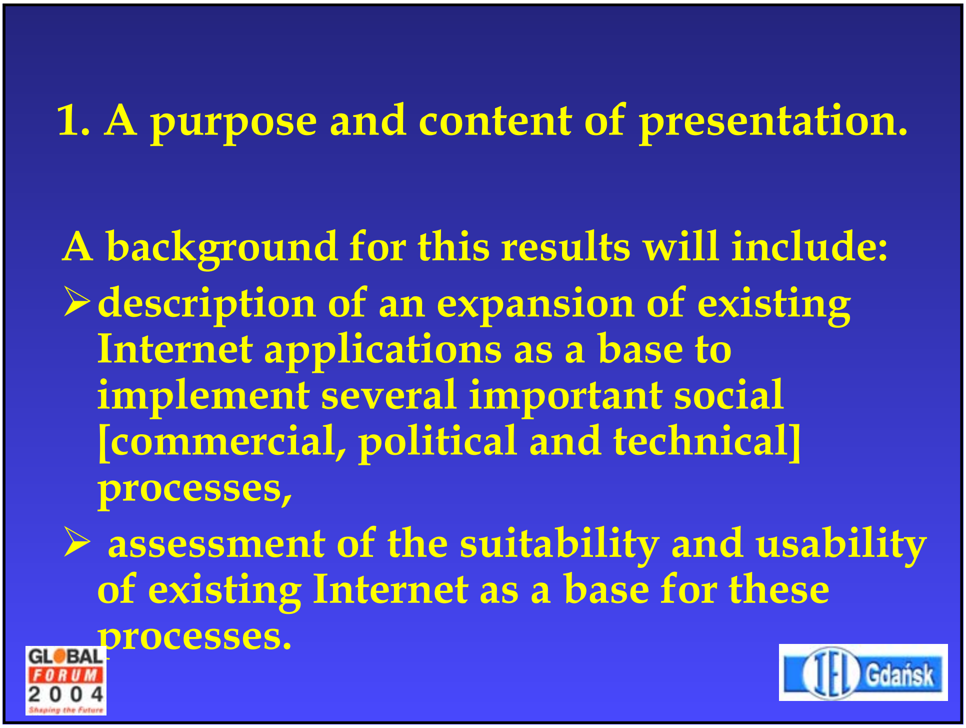
NOVEMBER, 4TH & 5TH, 2004
MALMÖ – SWEDEN



1. A purpose and content of presentation.

The purposes of the presentation include:

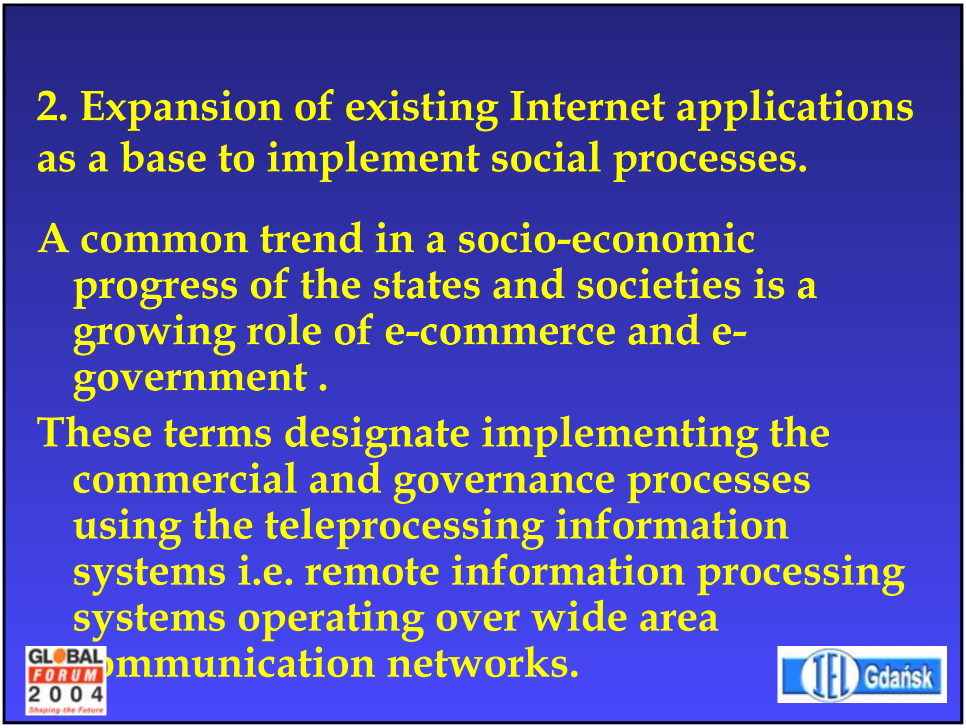
- to define a concept of “a secure Internet”,
- to describe basic features of “the secure Internet”,
- to formulate a proposal to establish a R&D project aimed at developing and launching a first version of “the secure Internet”.



1. A purpose and content of presentation.

A background for this results will include:

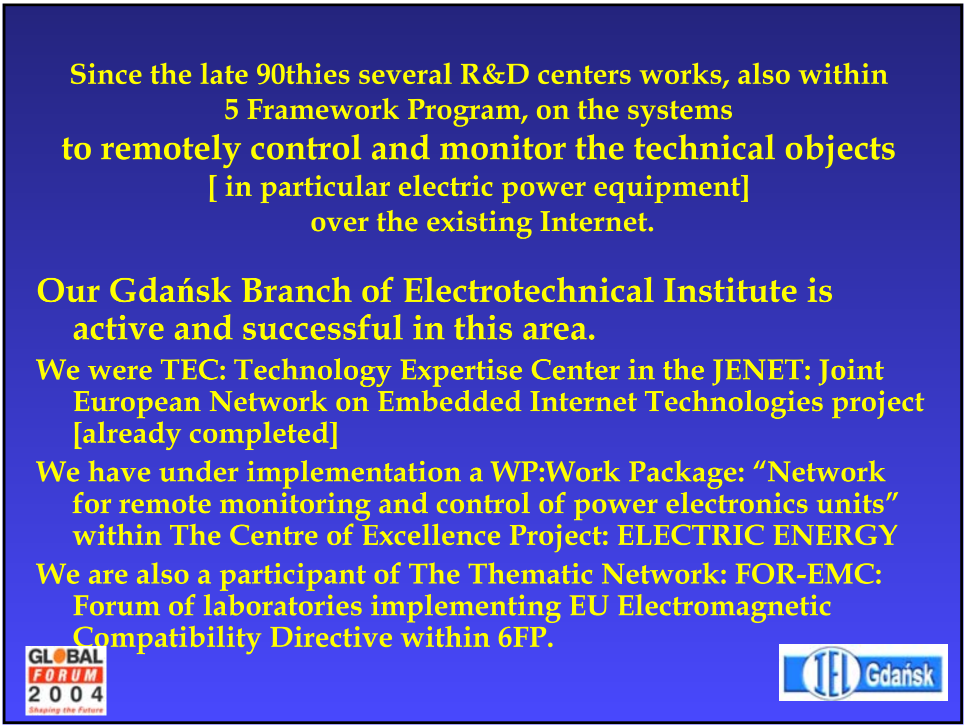
- description of an expansion of existing Internet applications as a base to implement several important social [commercial, political and technical] processes,
- assessment of the suitability and usability of existing Internet as a base for these processes.



2. Expansion of existing Internet applications as a base to implement social processes.

A common trend in a socio-economic progress of the states and societies is a growing role of e-commerce and e-government .

These terms designate implementing the commercial and governance processes using the teleprocessing information systems i.e. remote information processing systems operating over wide area communication networks.



Since the late 90thies several R&D centers works, also within 5 Framework Program, on the systems

to remotely control and monitor the technical objects

[in particular electric power equipment]

over the existing Internet.

Our Gdańsk Branch of Electrotechnical Institute is active and successful in this area.

We were TEC: Technology Expertise Center in the JENET: Joint European Network on Embedded Internet Technologies project [already completed]

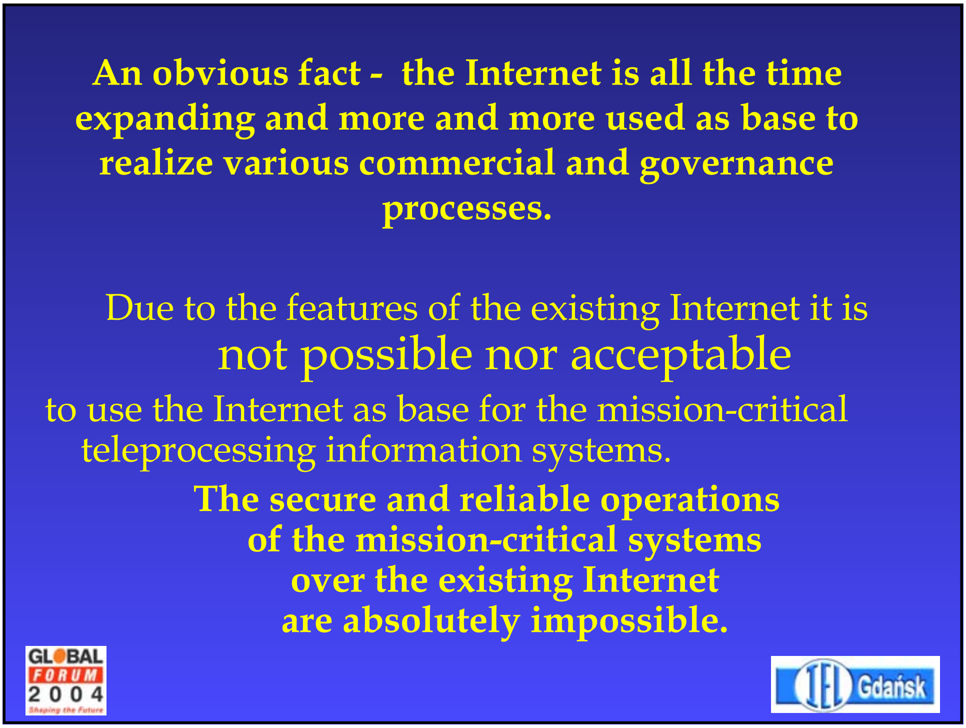
We have under implementation a WP:Work Package: “Network for remote monitoring and control of power electronics units” within The Centre of Excellence Project: ELECTRIC ENERGY

We are also a participant of The Thematic Network: FOR-EMC: Forum of laboratories implementing EU Electromagnetic Compatibility Directive within 6FP.

The mission-critical teleprocessing information systems

The teleprocessing information systems used for e-commerce, e-government and for control & monitoring.

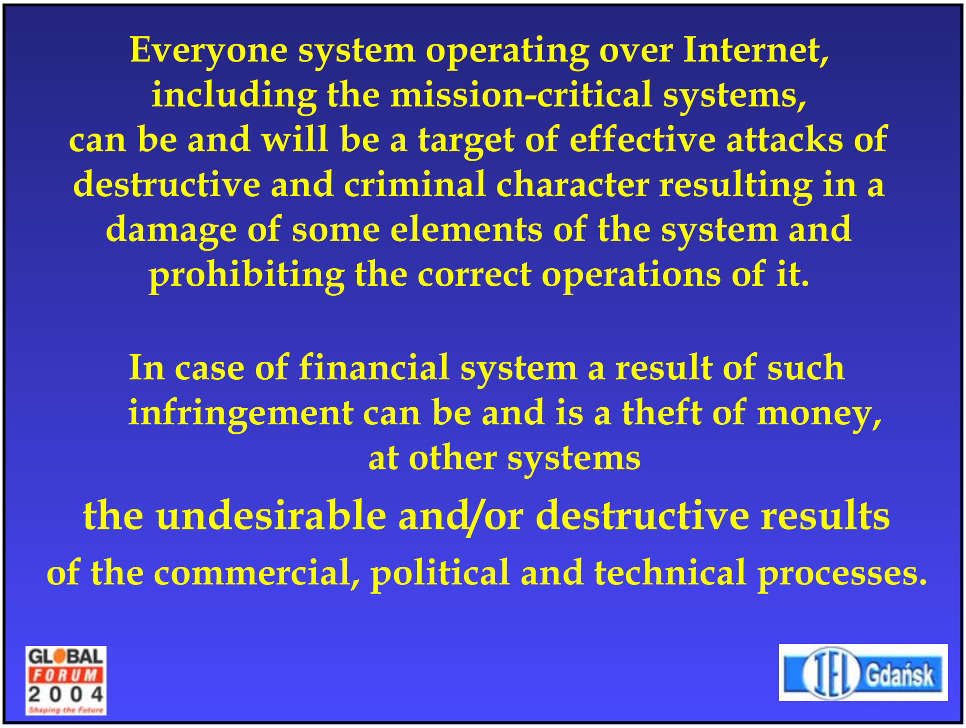
A popular opinion and believe is that the existing Internet is an adequate telecommunication base for e-commerce, e-government and technical control & monitoring i.e. an adequate telecommunication base for the mission-critical teleprocessing information systems.



An obvious fact - the Internet is all the time expanding and more and more used as base to realize various commercial and governance processes.

Due to the features of the existing Internet it is
not possible nor acceptable
to use the Internet as base for the mission-critical teleprocessing information systems.

The secure and reliable operations of the mission-critical systems over the existing Internet are absolutely impossible.



Everyone system operating over Internet, including the mission-critical systems, can be and will be a target of effective attacks of destructive and criminal character resulting in a damage of some elements of the system and prohibiting the correct operations of it.

In case of financial system a result of such infringement can be and is a theft of money, at other systems

the undesirable and/or destructive results

of the commercial, political and technical processes.

In spite of such situation the existing Internet is widely used to implement the commercial processes.

It results in occurring in the Internet the large-scale criminal activities.

These criminal issues are a subject of many reports.

The essential information on it

is contained in US government reports.

3. Lack of security at existing Internet and reasons for it according to US government reports.

A report prepared for Federal Trade Commission in September, 2003 states that in 2002 53 billion US dollars were stolen from bank accounts in USA using electronic & computer way.

Regular press messages report on viruses and other destructive operations in Internet which result in huge commercial loses, amounting to billions of US dollars.

The report „A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)”

published on January 21st, 2004

investigates usability of the existing Internet for e-government.

The report was commissioned by US Department of Defense.

It analyses a possibility to use the SERVE teleprocessing system supporting remote voting over Internet.

The „Executive summary” presents essential views and conclusions of the report :

“ This report is a review and critique of computer and communication
security issues
in the SERVE voting system,
an Internet-based voting system
being built for the U.S. Department of Defense's FVAP (Federal Voting Assistance Program).

The „Executive summary” presents essential views and conclusions of the report :

b. But in addition, because SERVE is an Internet- and PC-based system, it has numerous other fundamental security problems that leave it vulnerable to a variety of well-known cyber attacks (insider attacks, denial of service attacks, spoofing, automated vote buying, viral attacks on voter PCs, etc.), any one of which could be catastrophic.

The „Executive summary” presents essential views and conclusions of the report :

d. It is impossible to estimate the probability of a successful cyber-attack (or multiple successful attacks) on any one election.
But we show that the attacks we are most concerned about are quite easy to perpetrate.
In some cases there are kits readily available on the Internet that could be modified or used directly for attacking an election. ………….

The „Executive summary” presents essential views and conclusions of the report :

e. The vulnerabilities we describe **cannot be fixed by design changes or bug fixes** to SERVE.
These vulnerabilities are fundamental in the architecture of the Internet and of the PC hardware and software that is ubiquitous today

The „Executive summary” presents essential views and conclusions of the report :

e. It is quite possible that they will not be eliminated without **a wholesale redesign and replacement of much of the hardware and software security systems that are part of, or connected to, today's Internet.”**

Views and conclusions of the SERVE report are valid for every mission-critical teleprocessing system

– using the existing Internet as a base for such systems will result in catastrophic consequences and must not be accepted .

The conclusions of the report on SERVE are following:

- the Internet in the existing state is completely unusable as a base for e-government, e-commerce and technical control,
- within the architecture of the existing Internet it is not possible to provide for a required security and to eliminate the criminal activities – lack of security is a result of the most fundamental principles of operation of the existing Internet.

4. A new, secure Internet as necessary foundation for the mission-critical systems.

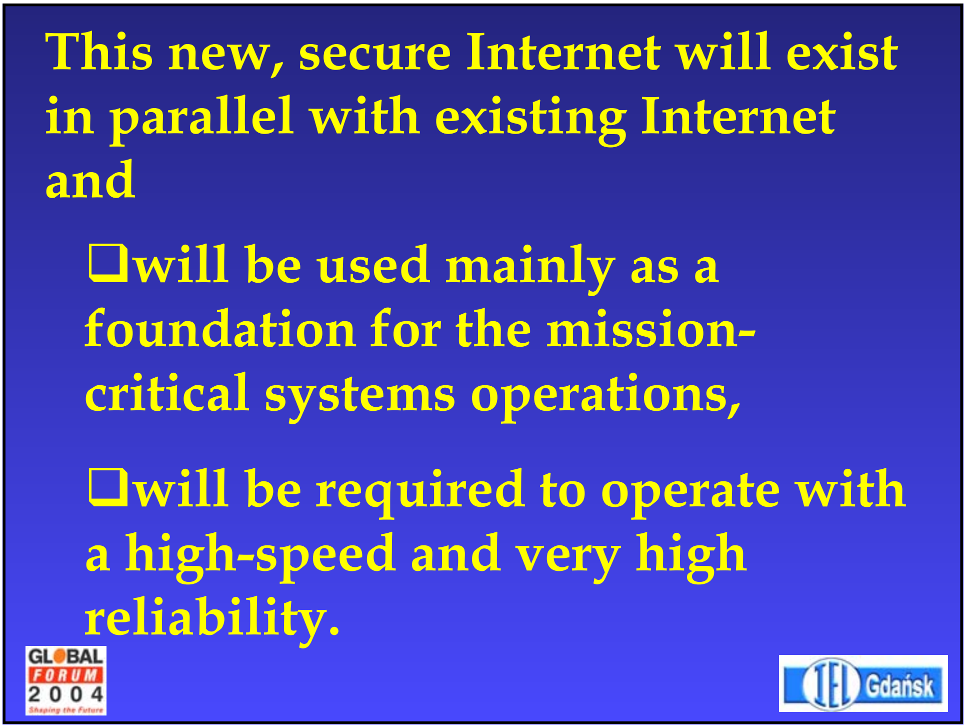
In the situation described
the only solution is to develop
a new, Internet-like, but secure
telecommunication network
to be used as a foundation
for the mission-critical systems,
to be called:

a secure Internet.

The secure Internet is to be a network which:

□will posses all advantages of existing Internet, a similar extent and ubiquity,

□will be free of the flaws and weaknesses of existing Internet,
will have an architecture and principles
of operations making criminal and
destructive activities
so difficult and dangerous
that almost unfeasible in practice.



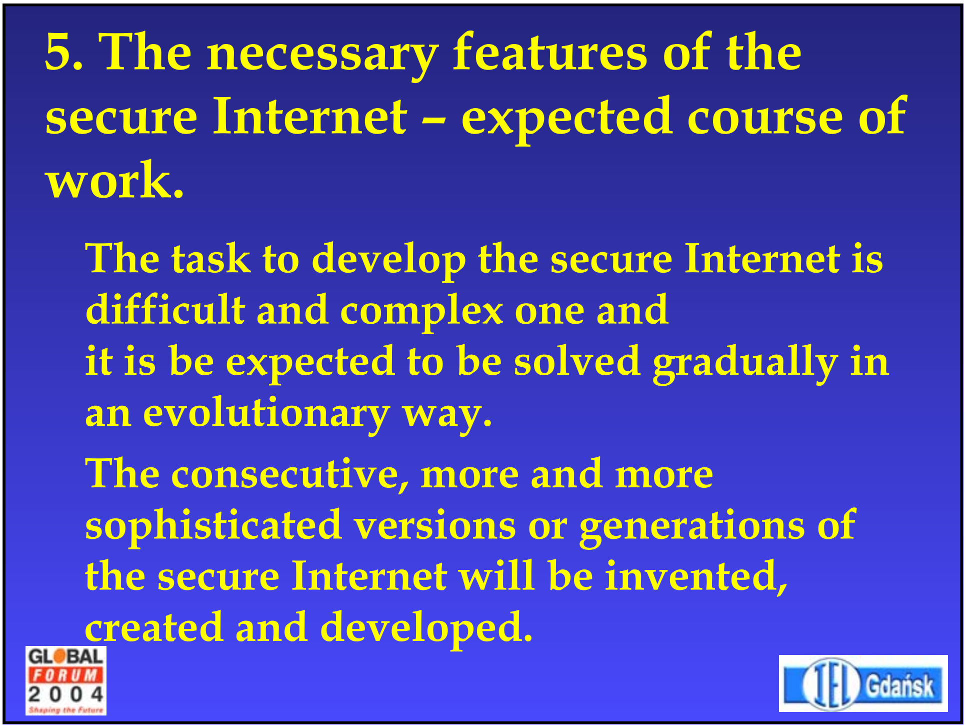
This new, secure Internet will exist in parallel with existing Internet and

- ❑ will be used mainly as a foundation for the mission-critical systems operations,
- ❑ will be required to operate with a high-speed and very high reliability.

To develop the new, secure Internet it is necessary to launch an adequate research, conceptual and design work.

Launching this work should be, in may opinion, recognized by an European and international community

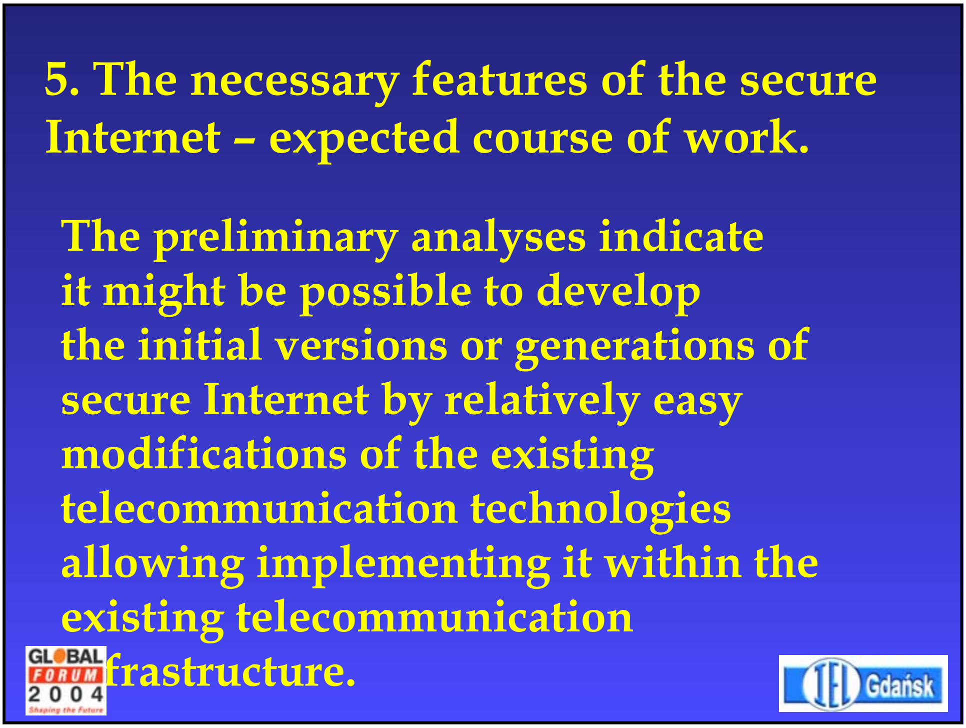
as key ICT research priority.



5. The necessary features of the secure Internet – expected course of work.

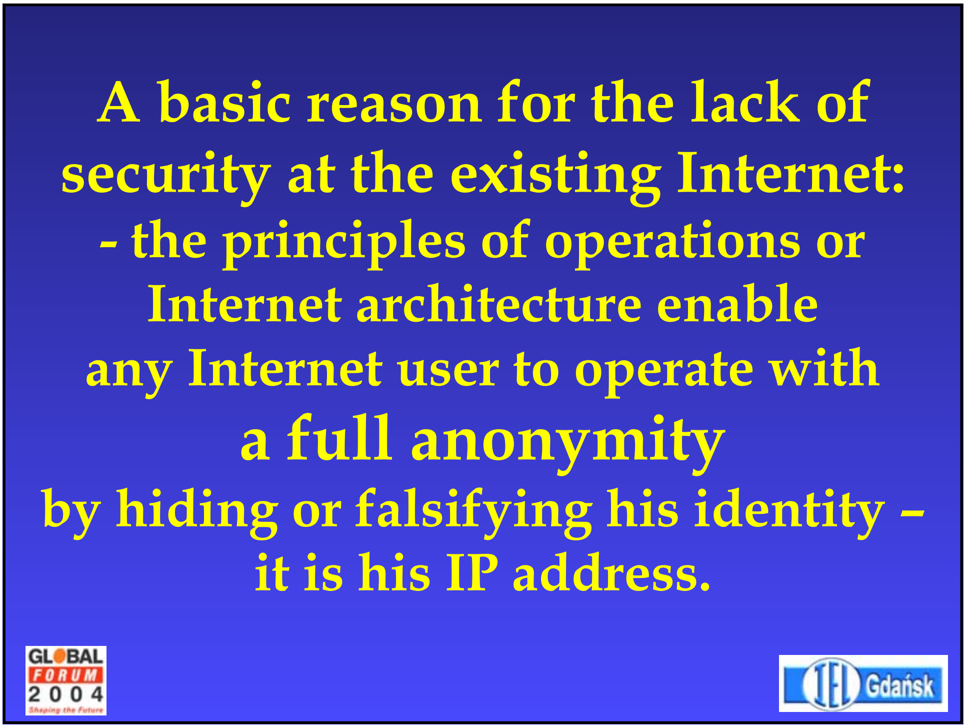
The task to develop the secure Internet is difficult and complex one and
it is be expected to be solved gradually in an evolutionary way.

The consecutive, more and more sophisticated versions or generations of the secure Internet will be invented, created and developed.



5. The necessary features of the secure Internet – expected course of work.

The preliminary analyses indicate
it might be possible to develop
the initial versions or generations of secure Internet by relatively easy modifications of the existing telecommunication technologies allowing implementing it within the existing telecommunication infrastructure.

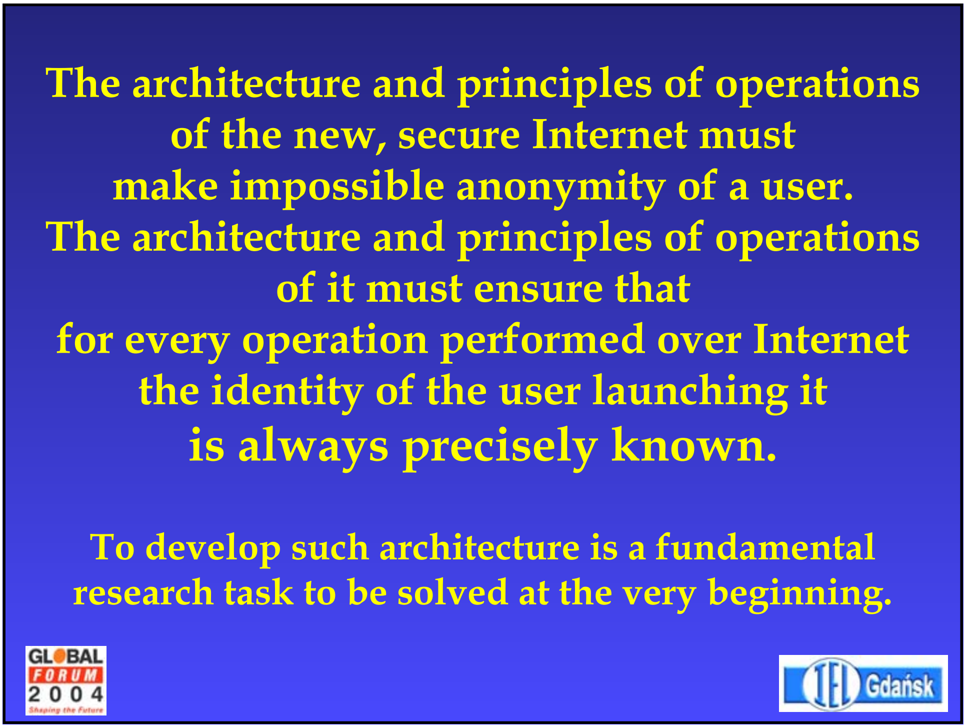


A basic reason for the lack of security at the existing Internet:
- the principles of operations or Internet architecture enable any Internet user to operate with

a full anonymity

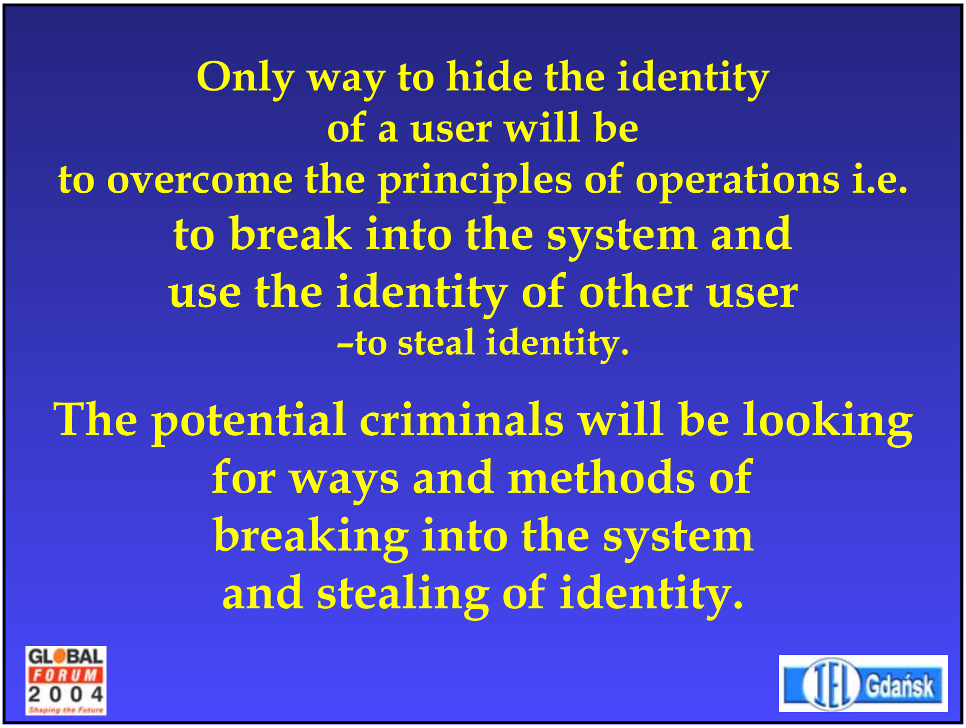
by hiding or falsifying his identity – it is his IP address.

GLOBAL FORUM 2004
Shaping the Future
IEL Gdańsk



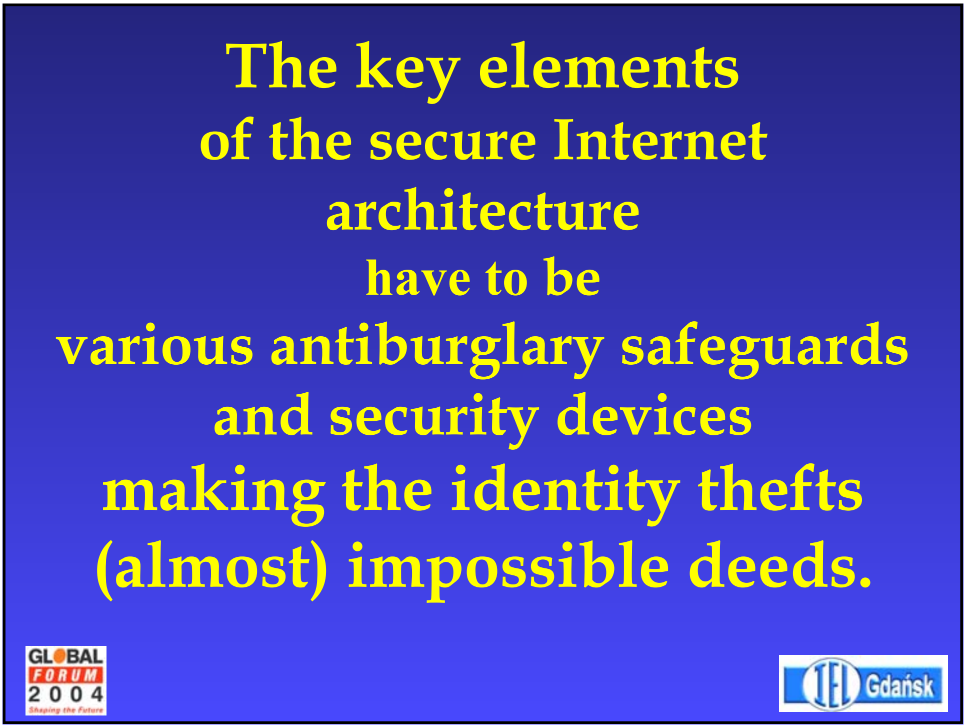
The architecture and principles of operations of the new, secure Internet must make impossible anonymity of a user.
The architecture and principles of operations of it must ensure that for every operation performed over Internet the identity of the user launching it is always precisely known.

To develop such architecture is a fundamental research task to be solved at the very beginning.



Only way to hide the identity
of a user will be
to overcome the principles of operations i.e.
to break into the system and
use the identity of other user
–to steal identity.

The potential criminals will be looking
for ways and methods of
breaking into the system
and stealing of identity.



The key elements
# of the secure Internet
architecture

have to be
various antiburglary safeguards
and security devices
making the identity thefts
(almost) impossible deeds.

It requires solving research tasks as:

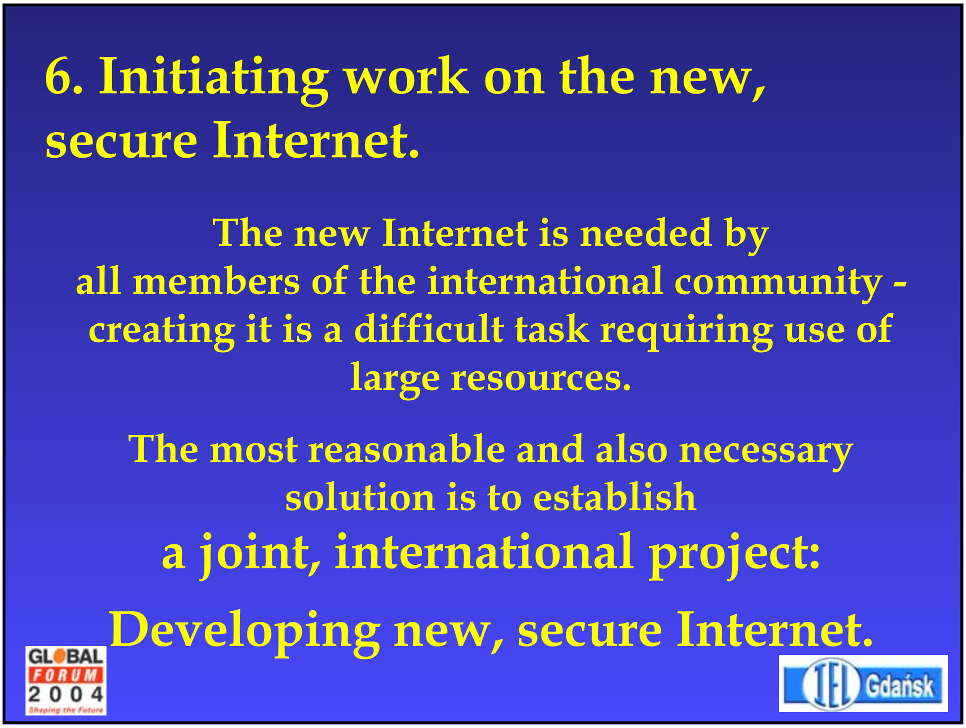
□ to analyse and identify the possible ways and methods of breaking into the network, with identification a level of danger involved,

□ to develop solutions neutralizing and closing the identified breaking ways and methods, at the first moment the most dangerous ones.

The work on the new Internet will take a long time.

Consecutive versions of the secure Internet architecture ensuring the higher and higher level of security will be created and developed.

Likely these evolution of architecture will involve increasing use of possibilities provided by the optical communication technologies.



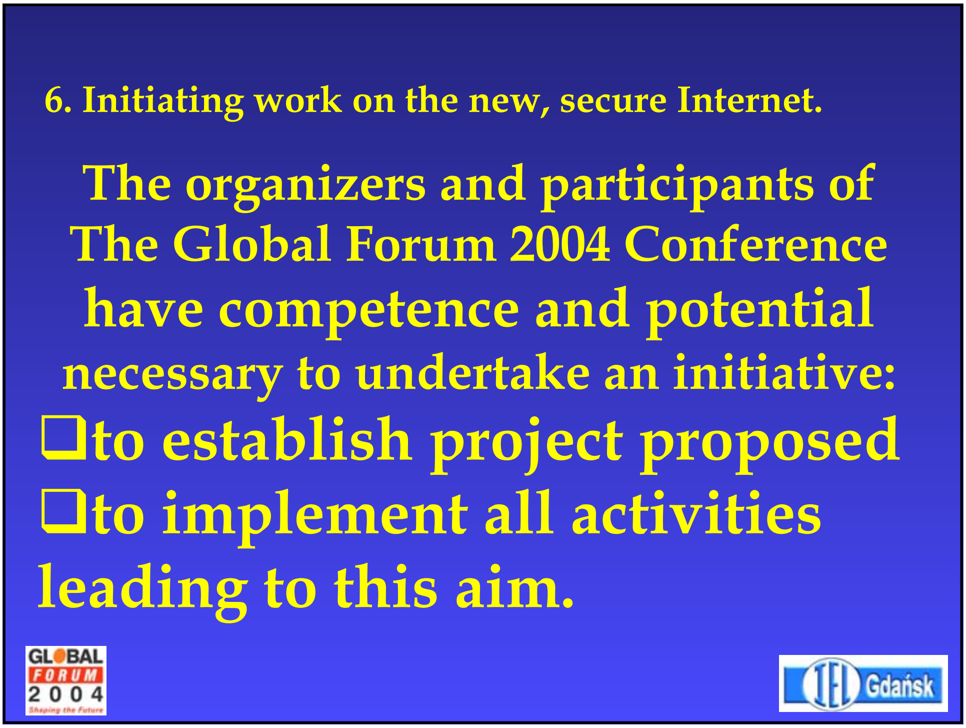
6. Initiating work on the new, secure Internet.

The new Internet is needed by all members of the international community - creating it is a difficult task requiring use of large resources.

The most reasonable and also necessary solution is to establish

a joint, international project:

Developing new, secure Internet.



6. Initiating work on the new, secure Internet.

The organizers and participants of The Global Forum 2004 Conference have competence and potential necessary to undertake an initiative:

❑to establish project proposed

❑to implement all activities leading to this aim.

Thank you for attention.

GLOBAL FORUM 2004 Shaping the Future

IEL Gdańsk