

**CYBER SECURITY PROBLEMS IN
ARCHITECTURE AND ORGANIZATION OF
SOUTH EAST EUROPEAN RESEARCH AND
EDUCATIONAL NETWORK (SEE REN)**

Eugene Nickolov

**National Laboratory of Computer Virology
Acad. G. Bonchev St. Building 8 Office 104
1113 Sofia, Bulgaria, eugene@nlcv.bas.bg**

1. History of SEE REN

The practical steps for development of a regional research and education data network in South East Europe (SEE) started in October 2000 in Thessalonica where GRNET (Greece) promoted a Memorandum of Understanding which was signed by INIMA (Albania), RoEduNet & RNC (Romania), UNICOM-B (Bulgaria), MARNET (FYROM), GRNET, AMREJ (Yugoslavia) and ULAKBIM (Turkey). Then a conclusion about the priority of developing a high-speed regional electronic network was made by the UNESCO/AE/ESF Expert Conference on reconstruction of the scientific cooperation in SEE in Venice in March 2001, and confirmed by the Round Table of the ministers of science of the Southeast European countries held in the framework of the 31st general conference of UNESCO in Paris on 24 October 2001. These ideas were further confirmed on the Ministerial conference in Sofia on 3 December 2001 and re-emphasized and extended with a clear intention towards the sixth framework programme on the "Workshop on Cooperation in Research, Science and Technology with the SEE-Countries within the framework of the SAP" in Bad Honnef in March 2002 and then on the high-level Conference at UNESCO, 4-5 April, and the Ministerial conference in Bucharest on 10th April 2002, where the necessity of creating a large bandwidth regional network was once more explicitly mentioned in the declaration. In May 2002 a workshop was held in Sofia on the Regionalization of National Research and Educational Networks (REN) in SEE. Its main decisions included elaboration of concrete projects for building linkages and cross-border connection among the neighbouring countries and exploration of the possibility to form a regional SEE REN on the organisational model of NORDUNet. The series of workshops organised by UNESCO-ROSTE, the German Commission for UNESCO, the Max-Planck-Institute for Physics and CERN aimed at the creation of a task force composed of the directors of the NRENs with the view of preparing of a regional project for development of the

electronic networks, and especially the formulation of a Letter of Understanding in Karlsruhe February 5th to 8th 2002.

The Main Conclusions of all these events could be outlined as follows:

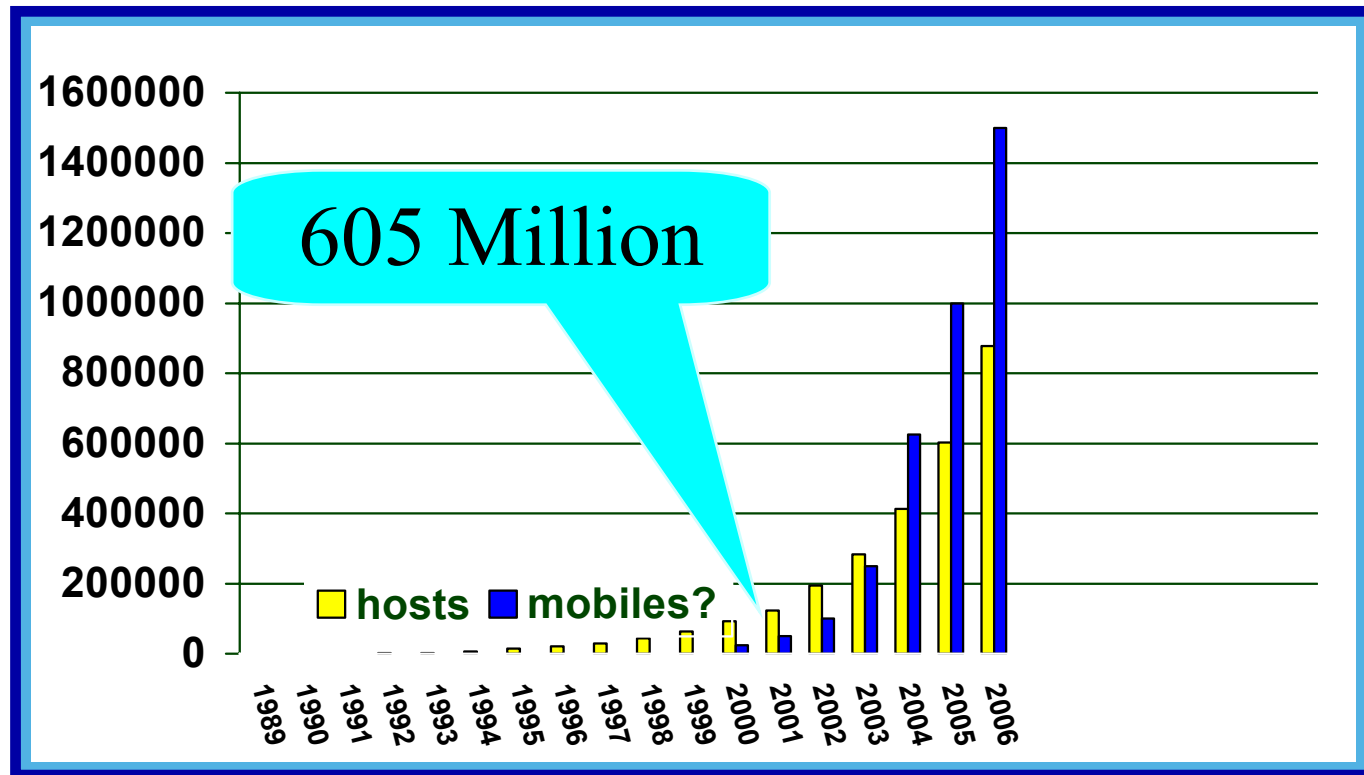
- A large-bandwidth regional REN, connected to GEANT, is the prerequisite for successful reconstruction of the scientific cooperation among the SEE countries and between them and the rest of Europe.
- Application projects that use the network should be developed together by the scientific communities and the national RENs.
- SEE RENs are promoting, with great effort, national connectivity of their academies, universities and other entities of research and education, but difficulties are regional networking monopolies and lack of infrastructure.
- Based on these conclusions the main objectives that would be achieved by the counties in SEE are:
 - Preparation of joint projects for the establishment of sustainable high-speed cross-border data connections, which will be the basis of the regional network.
 - Synergies between different new international lines and between the development of the national infrastructure and new lines.
 - Special projects on the content side, e.g. eScience, GRIDs and eLearning-projects, should complement this pure infrastructure project, which is the prerequisite for effective content development and scientific collaborations.

2. Present of SEE REN

When laying down the guidelines for the creation of SEE REN it is important to have in mind the main trends in the development of Internet:

- Higher speed backbones (10-40 Gbits/s per channel, up to 160 channels/fiber).
- Higher speed access (Gigabit Ethernet).
- Optical switching in the core.
- Wireless and mobile access (802.11a/b/g, 802.16, UWB, 3G/4G, Bluetooth, etc.).

The number of global internet host has grown dramatically in the recent years.



Source: CERT, based on www.nw.com, Jun 2000 + LM Ericsson
 Fig.1 Global Internet Hosts (000s) 1989-2006

2.1. The mission of SEE REN

One of the most important problems in front of the future SEE REN will be to establish an international service provider for the national REN. The main task is the implementation of connectivity between the national research networks and the General Internet. This could be realized in two ways: by peering with IP providers and by purchase of IP transit from IP providers. The lessons learned on the development of NORDUnet may be of great use. The implementation of a local connection by two providers instead of a transatlantic links might be cheaper and technically safer. The main issues will probably be the provision of stability and the challenges of the traffic growth.

The SEE REN will also act as a regional platform for scientific cooperation and as a part of the international research networking. Of course this will need a constant network architecture and organization development.

Today, in the light of the new realities and the major new threat to security not only of the citizens but of the very functioning of the national economies, the problem of the cyber security research and education is one of the most important. Obviously, it is only through the joint actions of governments and citizens directed by international organization as SEE REN that a reliable shield against cyber crime can be built.

The main activities of SEE REN may include:

- Research networking: SEE REN has to be built for peak load and use GÉANT for intercontinental connectivity.
- Network development: SEE REN could increase national activities and act as regional platform.
- Global Internet connectivity assuring the fast and effective accomplishment of different regional and international projects.

2.2 Organization and financing of SEE REN

The originators and the founders of the new regional network will be the regional state institutions, for example the national Ministries and Agencies of Science and Education as well as the academic institutions and universities, and the no-governmental organizations and no-profit associations. The managers of the regional REN will be members of the board of SEE REN.

Unfortunately most of the countries will not be able to construct the needed infrastructure by themselves and many promising projects will not be realized due to the lack of available funding. That's why SEE REN needs

international financial support and its development projects would have to be based on a cost-sharing basis, i.e. with contributions from local and international funds. Wherever possible, the deployment of projects has to follow well-established transparent tendering procedures. Although funds may exist there is currently no formal mechanism to link donors to the originators of ideas and vice versa. In the future SEE REN could act as a mediator between the national and international institutions and could identify novel arrangements that satisfy the requirements of research organizations and the donors.

2.3. Current problems in the international collaboration in SEE

They could be divided in three main groups: policy issues, technology issues and security issues.

The most policy issues are not specific for SEE. They include:

- The protection of intellectual property (trademarks, copyright, domain names, piracy).
- ICANN: Domain Names, IP Address allocation, dispute resolution.
- Online fraud and other abuses in e-commerce.
- Censorship (blocking web-pages and servers| and the problem of extra-territoriality and geographic independence.
- Taxation and double taxation.
- Security and privacy of information.
- Regulation, broadband, convergence.
- Cryptography and export controls.

The main technology issues are due to the degree of the development and the technical level of the RENs in the countries of SEE:

- In some countries RENs are very rudimentary.
- On average, regional RENs have 4-6 times less backbone capacity than RENs in the EU and NORDUnet and 20-30 times less access capacity (David Williams, CERN, NORDUnet Conference, Reykjavik, 24 August 2003).
- National infrastructures are not fully developed.
- High-speed internet connections between the regional capitals are not enough.
- The deployment of IPv6 standard is relatively slow.
- Domain name servers not fully internationalized yet.
- The broadband deployment should be accelerated.

The main security issues include:

- Reliability and Availability of data and systems.

- Security of Routers, DNS, Servers and Clients.
- Personal Privacy.
- Data Integrity and Confidentiality.
- Authentication of Parties in transactions.

2.4 Bulgarian participation

Recently were obtained:

- A considerable increase of the number of new computer systems for all strata of society (governing, education, science, private sector). The number of regular computer users in Bulgaria is growing all the time, having covered at the moment around 46 per cent of all citizens, mostly the young.
- A considerable increase of the Internet/Intranet connected new and relatively old computer systems. About 16% of the Bulgarians use regularly Internet. The Internet clubs are a favorite place for young people.
- A considerable increase of the average speed of Internet connection for the office and home computer systems. The building of an infrastructure among the Internet operators allows for an exchange of information at a speed of Gbps.
- A considerable increase of the number of secondary Internet Service Providers in terms of quantity and interconnectivity.
- A considerable improvement of academic and university Internet connectivity.
- Quite a success in building the legislative framework for fighting computer crimes.

The main non-solved problems include:

- A lack of national organization on governmental level coordinating and responsible for development of SEE REN.
- A lack of national strategy orientating the modest financial resources of the state in maintenance of the development of SEE REN.
- A lack of national action plan binding the national financing with existing and future international projects on regional level for the development of SEE REN.

The main needs of the scientific organizations which could be satisfied by the building of SEE REN are:

- Real time computing resources for solving problems in the field of mathematics (cyber security), physics, chemistry, biology and other scientific fields of study.

- Real time high speed communications for creating of virtual interdisciplinary research teams solving scientific and application tasks.
- Real time terabyte library arrays with different scientific profiles, offering well organized and correctly structured information for the national, regional and pan-European projects.

3. Future of SEE REN

The future of SEE REN is closely connected with the problems of the safety and security of networked information systems and the cyber security.

3.1 Cyber Security Paradigms:

- Possibilities vs. Security. No one country all over the world could meet alone the challenges of cyber terrorism. They demand a much greater potential than one isolated country has got. No matter what steps individual countries might take to safeguard their own critical information infrastructures, none of us will be secure until the least secure among us has addressed the issue. This technology gives us a shared opportunity, but also a shared vulnerability and a shared responsibility.
- Performance vs. Security. The “information society” is spreading globally, and it brings many benefits. The Internet is opening markets for small businesses, and e-government initiatives offer the promise of reliable and swift means of interaction between citizens and their governments. But the reliability and availability of these interconnected systems is threatened on a daily basis and it is very difficult to keep the whole possible performance together with the needed security.
- Private vs. Security. There is a tension between these desirable goals and it is always difficult to arrive at a compromise between protecting individual privacy and protecting society. Nowadays all over the world vulnerability increases as dependence grows on information technology and computer networking. Industry and academic communities need to take lead in securing systems – technologically and operationally.

3.2 Security Policy

3.2.1 Main Objective:

An IT security policy is aimed at protecting the confidentiality, integrity and availability of resources, data and programs. Essentially, it will:

- Define what the user wants to protect.
- Analyze what it is the user wants to protect it from.
- Explain how the user intends to protect it.

To be effective, the security policy must be both holistic and dynamic. To be achievable, it must be realistic in its goals and (where user conformity is required) expressed in a way that is simple and short enough to ensure it is understood and followed.

The overall security policy will address such areas as:

- Physical security of the data and systems.
- Access control to the data and systems.
- Data integrity and availability.
- Contingency and recovery plans.

Antivirus issues are simply one element of such a policy - viruses are one of the risks this policy must protect against.

3.2.2 Risk Analysis

A risk analysis outlines all the threats to the viability of the business. It examines the likelihood of each threat occurring and the impact of that occurrence. This allows the users to make informed decisions when assigning resources to manage the risk. Managing the risk might be achieved by controlling the vulnerabilities that expose the users to it (if the threat is highly likely to eventuate), or planning how to recover from it (if the threat is unlikely, but must be guarded against).

The risk analysis requires consideration of the following:

- Operating environment.
- Business systems.
- Threats.
- Impact assessment.

Each of these sections is covered in detail below.

3.2.2.1. Operating Environment

Here the environment within which the business operates is defined. This allows the IS manager to assess sources of vulnerability both within and to that environment. For the purposes of this paper, the list will be limited to the computing environment, as this is where the R&E network is vulnerable to viruses. The assessment will cover both the physical elements and the "control" issues of this environment. The following lists suggest areas to be considered:

3.2.2.1.1. Physical Elements

- Platforms (Intel, DEC, Macintosh, etc.).
- Operating Systems (DOS, Windows (all versions), NetWare, UNIX, etc.).
- Hardware (dumb terminals, diskless workstations, desktop systems, etc.).
- Software (off-the-shelf, customized, internally developed, non-business (e.g. games), etc.).
- Communications (network types, modems, and other links).

3.2.2.1.2. "Control" Issues:

- Standardization:
 - The level of server standardization.
 - The level of desktop standardization.
- Users:
 - The level of user competence in terms of security issues.
 - Controls that are in place to ensure and monitor staff conformity to security policy.
- Externals:
 - Definition of the reliance on contractors, solution providers, etc. (for hardware and software).
 - Definition of the reliance on external data and service providers (e.g. ISPs, stock-market feeds, etc.).
 - Definition of other external services and data that are accepted (news feeds, general downloads, etc.).

3.2.2.2. Research and Education Computer Systems:

Once a broad overview of the system is made, the IS managers may turn to the specific components of R&E system that need to be protected. Viruses directly threaten a computer system's data and computer based services and indirectly their reputation. Therefore, the task is thus to list all data and computer based services provided by or necessary to the computer system's existence. The list will include, but not be limited to, objects from the following areas:

- Internal Records:
 - Databases.
 - Spreadsheets.
 - Documentation.

- Product and Services information.
- Employee information.
- Strategic Plans (by category/department).
- Any other Sensitive and/or Confidential information (by category).
- Electronically Provided or Supported Services - Information services.
- External "Product":
 - "Data feeds" from external sources.
 - Access to external services.

3.2.2.3. Threats

A threat is a general danger to the viability of a computer system. As the discussion in this paper is confined to threats associated with malware, which primarily target R&E network's systems and data, the threats may be limited to the following:

- Threats to data.
- Threats to systems (software, communications, services).
- Threats to reputation.
- Threats to finances.

In the wider scheme of things, all of the ways the above areas are threatened have to be listed. Thus, while the focus is on the threat to the data from viral incidents, normally IS managers would also identify the data being vulnerable to damage by anything from a major disaster, such as a fire or flood, through more common occurrences, like a hard drive failure, faulty cable, power interruption and simple user error. It is not enough to identify the susceptibility of the systems to a malware attack as vulnerability – IS managers also have to understand how malware gains access to their systems, so that they can take measures to keep them out. The pre-work in defining the operating environment can help here - it limits the list of vulnerabilities to those that target that environment.

This is the final piece of the risk assessment. Having identified what the business areas are, and the threats to those areas, IS managers now need to determine what impact it will have on the business if one of these areas is compromised. Some of the possible "damage" categories are listed across the top of Figure 2. The actual impact assessments are purely notional - they will vary by company.

Object	If destroyed	If altered/ corrupted	If exposed	If suspended
Customer database	Medium (restore from backups)	High (are backups corrupted?) (Cost if change undetected?)	High (damage reputation/ market edge)	Medium (Interrupt s work)
Software package X	Medium	High	High (if proprietary)	Medium
Web site general info	Medium	High	NA	Medium
Web site order entry page	Medium	High	NA	Medium
Access to external data	NA	High	NA	Medium

Figure 2: Impact Analysis

A true risk analysis would also include some indication of the size and type of investment an object represents, and its "replaceability" should it be lost, along with the general impact assessment. The depth of analysis required for this section will be governed by the complexity and needs of the business. Where different business units come to different impact assessments on the same object, the IS manager should always record the highest impact.

3.2.3. Definition of the Security Baseline and the Additional Security Measures

The baseline defines the minimum security implementation. For simple ease of management, it would be ideal if a single baseline for the entire computer network could be defined and implemented; in practice, the number and diversity of systems and units may make this impossible. The baseline will derive from the information discovered in the risk assessment, and may require changes to the operating environment.

Additional security measures aim at controlling the "high-risk" areas of the network identified in the risk analysis. These may address applications that have been identified as open to particular attack, mission-critical units, and responses to particular types of threat. Clearly the distinction between the

security baseline and additional security measures will be highly specific. Any of the alternatives may be reserved as additional security measures, just as the additional controls could be implemented as part of the security baseline. Some specific risks that will be managed by the additional security measures include:

- Laptops/mobile users (unless tightly controlled exist outside the security perimeter).
- Researcher/Students/Service personnel, etc.
- Downloaded software.
- Disks, programs, documents brought from outside the office.
- Unauthorized software.
- Deliberate attack.

3.2.4 Security Procedures Document

While a security solution may be largely imposed through a policy driven selection and implementation of hardware and software, it will always include behavioral elements as well. The procedures document outlines the expected behavior of the users within the system. As such it must be concise, simple to read, and easy to understand. Ideally it will be backed up with a comprehensive awareness campaign that delivers enough knowledge on the problem and the policy and solutions to it, to ensure the users are correctly playing their role in meeting this security threat. Clearly, there may be a number of sections to the procedure document, each targeted at the next level of responsibility within the computer network.

A basic procedures document will outline what users can (and cannot) do on the system, as well as the procedure to follow if they know or suspect they have a malware outbreak. It will consist of at least some of the following elements:

- Outline of prohibited actions (e.g. no games, disks, modems; no altering desktop, etc.);
- Outline of required actions (e.g. scan all disks, downloads, etc.);
- Outline of reporting procedures (when and what to report, and to whom);
- Outline of incident response and escalation strategies (what the help desk is to do if an incident or suspected incident is reported);
- Review strategies (what will be done if the system fails).

The ultimate aim here is to make users irresponsible - they have to report suspicious behavior to the appropriate source. This has the double advantage of raising the probability that malware incidents will be discovered early

while preventing a flood of hoax messages, by ensuring they are forwarded to the appropriate point and nowhere else.

3.2.5 Security Awareness Plan

The awareness plan will be a plan of action to raise users understanding of the risks the network is exposed to and how their actions can affect that exposure. It may include:

- Basic introduction to how malware work, or at least to the actions that can introduce malware.
- Introduction to the extended malware problem, discussing issues such as DoS, virus, Trojan horse etc. attacks.

Explanation of the security strategy adopted by the unit:

- The tools available to them.
- The procedures they must follow.
- Outline of the disciplinary or corrective measures that will be taken should the above procedures be violated.

3.3 South East Europe Cyber Security Conference

In September the government of Bulgaria, US Department of State, USAID and Internews organized in Sofia, Bulgaria a Conference on the Cybersecurity, which was aimed at ensuring the safety and security of networked information systems. The participation of Albania, Bosnia and Herzegovina, Croatia, Czech Republic, Hungary, Macedonia, Moldova, Montenegro, Poland, Romania, Serbia, Slovakia, Slovenia, Ukraine, Council of Europe, European Commission and USA demonstrated the importance of the problem and the willingness of the countries to secure their national critical information systems and thereby enhance their security and that of the global information networks on which we all rely.

The main topics of the conference were:

- Organizing to secure critical information infrastructures - processes, challenges and lessons learned.
- Trends in threats to network information systems.
- Cybercrime legislation and legal reform.
- Cybercrime law enforcement capabilities and capacity building.
- Public-private partnerships and information sharing.
- Cyber incident watch, warning and information sharing.
- Approach to securing networked information systems.
- Regional approach to cyber security.
- South East Europe Cyber security cooperation – issues for consideration and way-ahead.

One of the most important decisions was about the creation of a regional centre of cyber security cooperation – an initiative of the Bulgarian president Georgi Purvanov. This centre is conceived as a non-governmental organization that is to work for preventing and minimizing the risk of cyber crimes. The Center will be training representatives from the countries of Southeast Europe, judges, prosecutors, investigating magistrates and policemen in the general and special problems of the European law enforcement practices in fighting computer crimes. The Center will also conduct research and develop projects designed to give early warning about the appearance of new cyber threats, viruses, possible hacker attacks, etc. The early warning of a new virus could reduce substantially the cost of overcoming the effects of its harmful actions.

4. Conclusions

There is no country that, in the age of Internet and cyber terrorism, can remain indifferent or rely, as earlier, on nature or geography to develop self-dependent economics and protect it single-handed against malicious acts. Besides bringing people closer, the Internet has eliminated distances and differences while placing at the hands of many people a very powerful means of organized acts. SEE has to make the necessary arrangements to join the western countries and to reach a common electronic identity towards different services.

What is needed to realize fully and in reasonable terms the idea for SEEREN in?

Smoothing away contradictions and achieving inter-acceptable compromises between the states and the respective representing organizations; and providing of necessary financing on national and European level.