

**Cyberwar ante portas: Exploiting the
role of the academic community
in national cyber defense exercises**

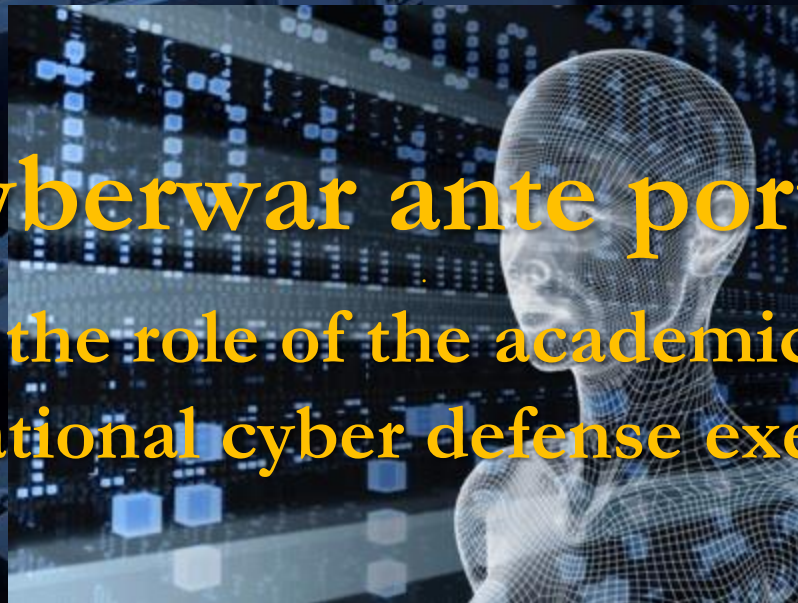
Dimitris Gritzalis

September 2010

Invited talk: 5th International Conference on Critical Information
Infrastructure Security (CRITIS-2010), Athens, 2010

Cyberwar ante portas!

Exploiting the role of the academic community
in national cyber defense exercises



Professor Dimitris Gritzalis (www.cis.aueb.gr)

**Member, Cyber Committee PANOPTIS-2010
& Coordinator of Academic Institutions**

**Director, Information Security & Critical Infrastructure Protection Research Group
Dept. of Informatics, Athens University of Economics & Business (AUEB)**



Truths (or not?)

“Microsoft has vast resources, literally billions of dollars in cash or liquid assets reserves.

Microsoft is an incredibly successful empire built on the **premise of market dominance with low-quality goods**”

Richard A. Clarke

Cyber War: The Next Threat to National Security and What to Do About It



Cyber Attack and Cyber War

Cyber Attack is every illegal action, which takes place through the use of computers and electronic networks, and results in the disruption or degradation of services, in order to upset the public and affect the population of a country or the state, and force them to accept specific political, social, or ideological objectives.

Cyber War is the use of computer and computer networks – and mainly the Internet to conduct war in the cyber space, which is *declared*, based on a protocol that classifies specific cyber attacks as actions of war, and is conducted - mainly but not only - through the use of cyber attack/cyber defense.



MS-ISAC OPERATIONS CENTER



Top 10 Ports Under Attack

9988
2443
2398
2882
2984
4062
4476
41170
3393

DHS/ISAC Threat Levels

Current Cyber Alert Levels

MS-ISAC ↓ **LOW**

IT-ISAC ↓ **LEVEL 1** SANS ↓ **LEVEL 1**

FS-ISAC ↓ **LOW** SYMANTEC ↓ **LEVEL 1**

Current Physical Threat Levels

DHS **ELEVATED** FS-ISAC **ELEVATED**

Top 10 Attacking IPs

216.120.067.226
061.129.033.110
195.060.099.211
210.004.137.219
211.106.172.001
202.062.224.090
150.164.029.259
121.015.253.104
061.170.085.077

Latest Viruses, News and Advisories

Microsoft Internet Security and Analytics Center Advisories

83 Items - mouse over list to scroll

new vulnerability in java could allow for remote code execution
 Vulnerability in Adobe Flash Player Could Allow Remote Code Execution
 Sun Java Runtime Environment and Java Web Start Remote Code Execution
 Vulnerabilities in Microsoft .NET Framework Could Allow Remote Code Execution
 Multiple Remote Code Execution Vulnerabilities in Internet Explorer
 Multiple Remote Code Execution Vulnerabilities in Internet Explorer
 Security Vulnerability in Novell GroupWise



About the MS-ISAC Digital Dashboard

The Digital Dashboard was developed by the MS-ISAC as a central resource to provide valuable, real-time data regarding the current cyber security environment. The Dashboard features a variety of sources, including cyber attack information, cyber alert threat levels, and the latest advisories and news to assist organizations in their cyber security efforts. Comments can be directed to isac@cscic.state.ny.us

US Time Zone Information

Hawaii	Alaska	Pacific	Mountain	Central	Eastern



[text version](#) | [help & how to...](#)

Cyber Defense: The role of the State

Role?

- ➡ Duty for national **critical infrastructure** protection
- ➡ Plan, defend, and react against (**mainly large**) **scale attacks**
- ➡ Promote and support **awareness, prevention, and training**
- ➡ Support **Research & Technological Development**

Why?

- ➡ Availability of required **resources**
- ➡ Access to the required **know-how**
- ➡ Legal right to **coordinate** actions, on a **national** level
- ➡ Legal right to act **proactively**

Cyber Defense: The role of academic community

Role?

- Supply **state-of-the-art technology**
- Participate to **cooperation activities**, on a national level
- Focus on **research and development** activities
- Promote **awareness** and timely **training** of new scientists

Why?

- Contribute to the **National Security**
- Organize and support **Centers of Excellence**
- Carry out **assess** and **evaluation** activities
- Exploit and improve international **academic cooperation**

National cyber defense exercises: Why?

- ✓ **Promote public awareness**, clarifying the real dimension of the threat, without exaggerations or oversimplifications.
- ✓ **Train** involved staff, so they can **detect attacks** in time and **limit** the impact of a cyber attack against an infrastructure.
- ✓ **Improve the coordination, communication, and cooperation** between public and private stakeholders.
- ✓ **Evaluate and assess** the national strategic plan for dealing with cyber threats.



Generic principles of the academic community

- 
1. **Working together with all involved parties**
(The target is the cooperation – not the competition among individuals/institutions)
 2. **Open and synergetic procedures**
(Utilizing all available resources – no exclusions and no discriminations)
 3. **Multilateral communication and support**
(All parties involved support each other – no one-way activities)

PANOPTIS 2010

1st National Cyber Defense Exercise

18-20 May 2010

Academic and Research Institutions Team

Coordinator: Prof. Dimitris Gkritzalis (AUEB)



(X+Y): X Professors, Y Researchers/Network Admins
Players: 14 Universities, 4 Technological Institutes,
3 National Research Institutes, 2 National Commissions
Totals: 85 Experts (31 Professors, 54 Researchers)

Inventory of experts: A corner stone

Specification of an inventory of experts

Identification and registration of experts and their skills

Exploitation of the existing expertise

CBK: Information Security & Critical Infrastructure Protection
Prerequisite Knowledge, Basic Terminology and Security Models
Access Control and Authentication
Cryptography
Network, Web and Communications Security
Database Security
Software Security
Information System Security Management
Ethical, Social, Psychological and Legal Issues
Forensics
Physical Security and Critical Infrastructure Protection

Domain of Expertise: (8) Forensics	
Sub-Domains	Notes
8.1 Steps	
8.2 Data Collection	
8.3 Network & Web Forensics	
8.4 Database Forensics	
8.5 Hardware Forensics	
8.6 Data Usage Prerequisites	
8.7 Psychology	

Domain of Expertise: (6) Network, Web and Communications Security	
Sub-Domains	Notes
6.1 Network Security Protocols	
6.2 Wireless Network Security	
6.3 Distributed Systems	
6.4 Secure Networking	
6.5 IDS and Malicious Software Protection	
6.6 Security Network Technologies	
6.7 Special Purpose Network Systems	
6.8 Legal Issues	

PANOPTIS 2010 - Attack scenarios (1/3)

1. **Distributed DoS Attack:** Players were asked to defend against a SYN flooding attack, which initially targeted a single organization, but soon affected a large number of systems/organizations.
2. **Spear-Phishing email Attacks:** Malicious Spoofed emails were send to specific targets, asking them to perform certain actions and/or containing malicious payloads. Players had to identify and report the malicious emails.
3. **Incident Handling:** A disk image of a compromised Linux system was given for analysis to the players. The objective was to detect the actions performed by the attacker.



PANOPTIS 2010 - Attack scenarios (2/3)

4. **Data Leakage:** Players were asked to analyze a suspicious email and detect if the message or its contents contained hidden sensitive information.
5. **Web Hacking:** Players were asked to deploy a well-known open-source application and harden it. Later on, this system was attacked by the Red Team to test the player's defenses.
6. **Web DoS:** Players were asked to install a well-known Web Server and harden against DoS attacks. Later on, this system was attacked by the Red Team to test the player's defenses.

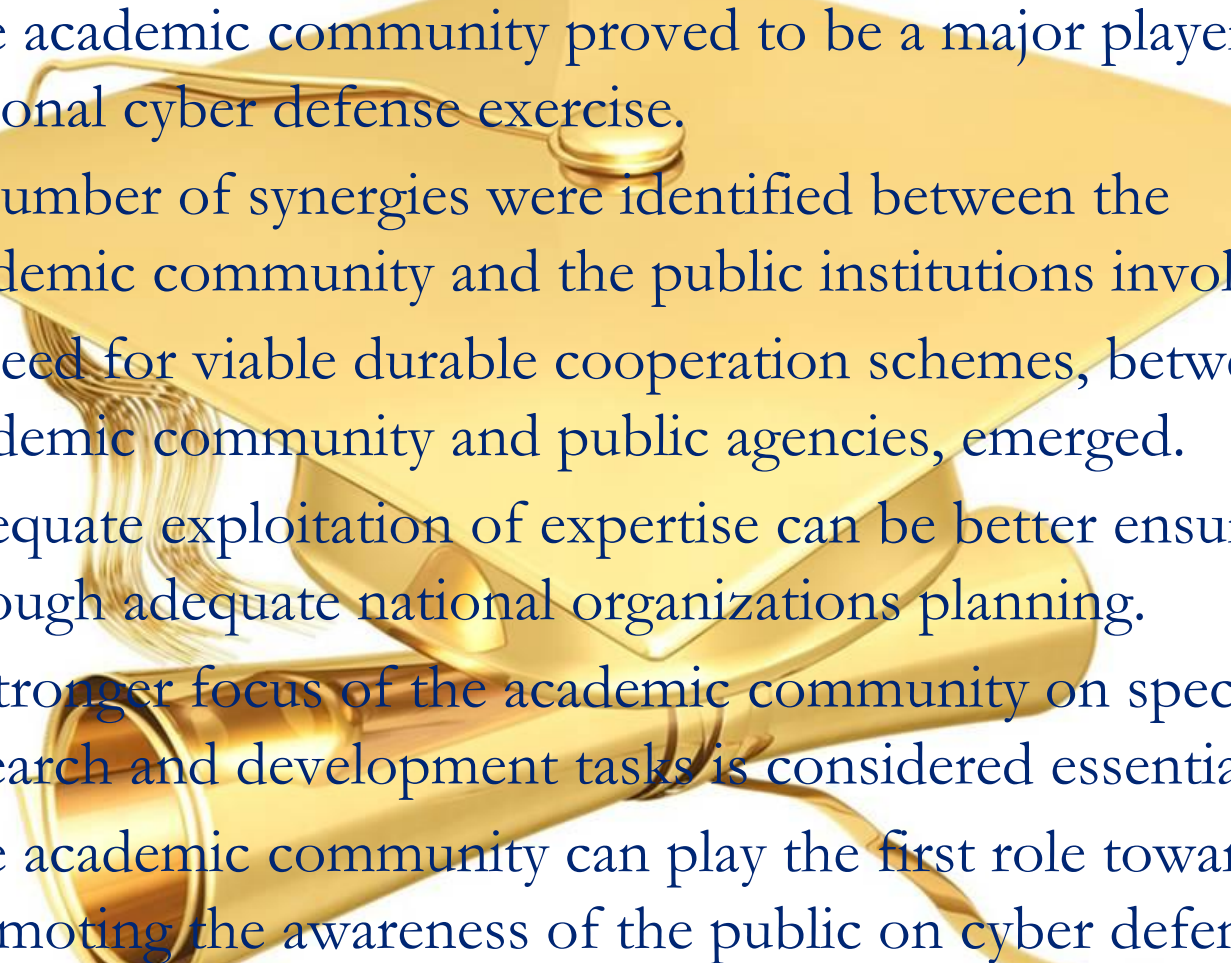


PANOPTIS 2010 - Attack scenarios (3/3)

7. **Malware Analysis:** Two types of malware (one well-known and one proprietary) were given to the players, who were asked to analyze them and report their actions.
8. **Legal Conflict:** The legal team of the players were asked to analyze a hypothetical - still realistic - legal conflict.
9. **Web Defacement/System Misconfiguration:** A vulnerability of a popular application server was exploited, allowing an attacker to gain access to the system. Players were given the web and application servers logs, and asked to identify the vulnerability and propose corrective actions.



Some preliminary conclusions

- 
- The academic community proved to be a major player in a national cyber defense exercise.
 - A number of synergies were identified between the academic community and the public institutions involved.
 - A need for viable durable cooperation schemes, between academic community and public agencies, emerged.
 - Adequate exploitation of expertise can be better ensured through adequate national organizations planning.
 - A stronger focus of the academic community on specific research and development tasks is considered essential.
 - The academic community can play the first role towards promoting the awareness of the public on cyber defense.

References

1. Denault, M., Gritzalis, D., Karagiannis, D., Spirakis, P., "Intrusion detection: Evaluation and performance issues of the SECURENET system", *Computers & Security*, Vol. 13, No. 6, pp. 495-508, 1994.
2. Doumas, A., Mavroudakos, K., Gritzalis, D., Katsikas, S., "Design of a neural network for recognition and classification of computer viruses", *Computers & Security*, Vol. 14, No. 5, pp. 435-448, 1995.
3. Dritsas, S., Tsoumas, B., Dritsou, V., Konstantopoulos, P., Gritzalis, D., "OntoSPIT: SPIT Management through Ontologies", *Computer Communications*, Vol. 32, No. 2, pp. 203-212, 2009.
4. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D., "An Insider Threat Prediction Model", *Proc. of the 7th International Conference on Trust, Privacy, and Security in Digital Business*, pp. 26-37, Springer, Spain, 2010.
5. Katsikas, S., Gritzalis, D., Spirakis, P., "Attack Modeling in Open Network Environments", *Proc. of the 2nd Communications and Multimedia Security Conference*, pp. 268-277, Chapman & Hall, Germany 1996.
6. Katsikas, S., Spyrou, T., Gritzalis, D., Darzentas, J., "Model for network behaviour under viral attack", *Computer Communications*, Vol. 19, No. 2, pp. 124-132, 1996.
7. Tsoumas, B., Gritzalis, D., "Towards an ontology-based security management", *Proc. of the 20th International IEEE Conference on Advanced Information Networking and Applications*, pp. 985-990, IEEE, Austria 2006.
8. Virvilis, N., Dritsas, S., Gritzalis, D., "Secure Cloud Storage: Available Infrastructure and Architecture Review and Evaluation", *Proc. of the 8th International Conference on Trust, Privacy & Security in Digital Business*, pp. 74-85, Springer, France 2011.
9. Virvilis, N., Dritsas, S., Gritzalis, D., "A cloud provider-agnostic secure storage protocol", *Proc. of the 5th International Workshop on Critical Information Infrastructure Security*, pp. 104-115, Springer, Greece 2010.