Academic Research on Cybersecurity

BULGARIAN
ACADEMY
of SCIENCES
1869

Todor Tagarev, Zlatogor Minchev, Nataliya Ivanova

IT for Security Department, Institute of ICT, Bulgarian Academy of Sciences

IICT

Sixth Scientific Conference of the International Information Security Research Consortium

October 1-2, 2012

Sofia, Bulgaria, Park Inn Renaissance

IT for Security Department

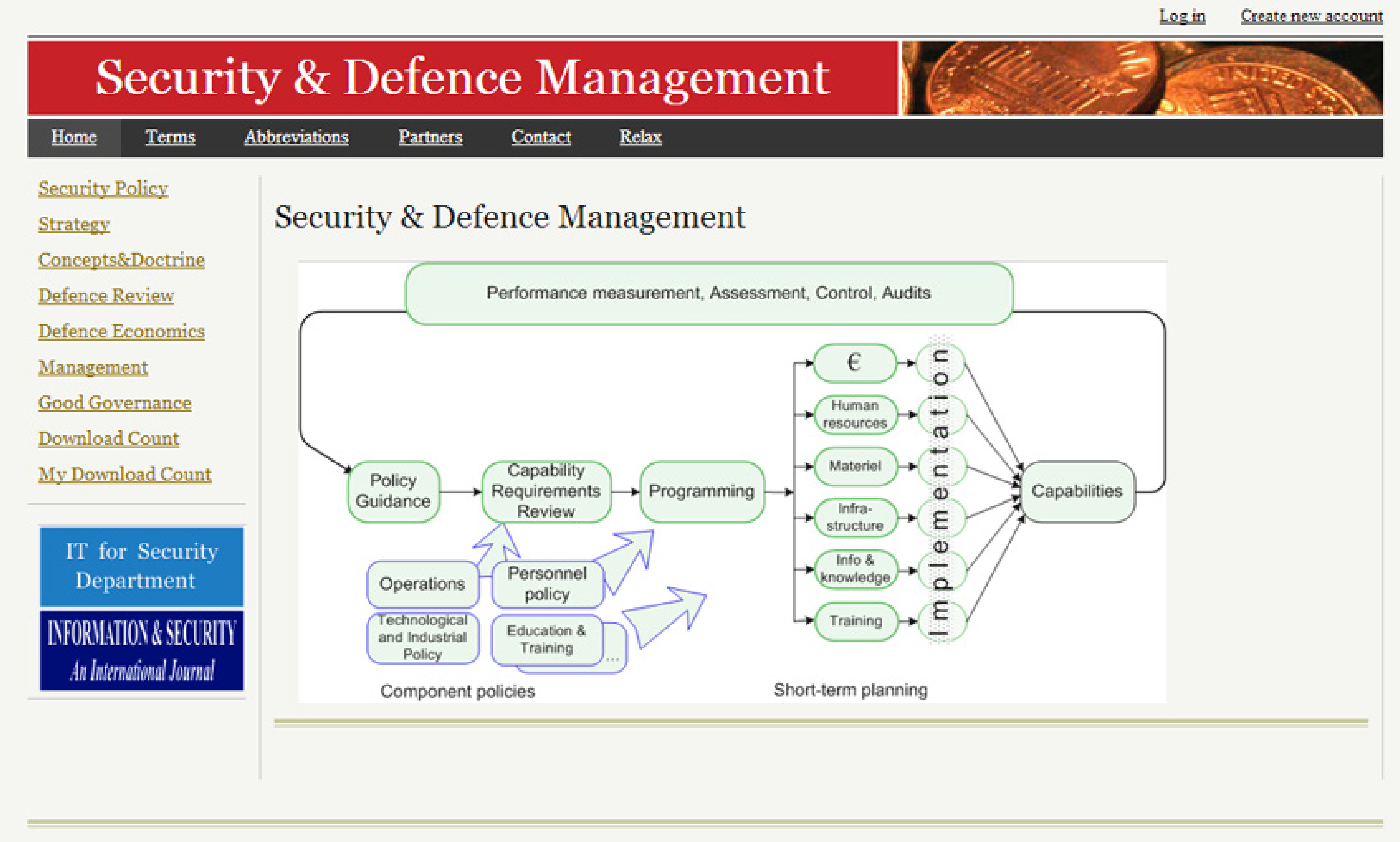
- Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, http://iict.bas.bg
- IT4Sec Department, www.IT4Sec.org
- CSDM & Strategic Security and Defence Management site, www.defencemanagement.org
- Joint Training, Simulation and Analysis Centre
- “Information and Security” journal

Outline

- Requirements (expectations) to academic research on cybersecurity
  - Policy support
  - Technologies
  - Support to education and training
  - Knowledge dissemination
- Academic research in Bulgaria and partner networks
- Discussion

Policy support

- Awareness of cyber risks and threats
- Defining capability requirements and assignment of responsibilities
- Defining ‘Rules of Engagement’
  - Including preservation of human rights and freedoms
- Coordination & Cooperation
  - Operations, Training
  - Capabilities development
- Allocation of resources
- Provision of transparency, accountability, integrity



Security & Defence Management

http://defencemanagement.org/

Specific topics

- Assigning cybersecurity responsibilities in the national security sector
  - Analysis of alternatives
- National roles and specialization in the framework of NATO and the European Union
  - Management of the scientific and technological ‘infrastructure’

Cybersecurity Knowledge Management

- Definitions
- Policies
- Strategies
- Organisations & Responsibilities
- Cyber Threats
- Cyberwar & Cyberdefence
- Standards & Technologies
- Education & Training
- Research Centres
- Studies
- Democratic oversight & human rights and liberties

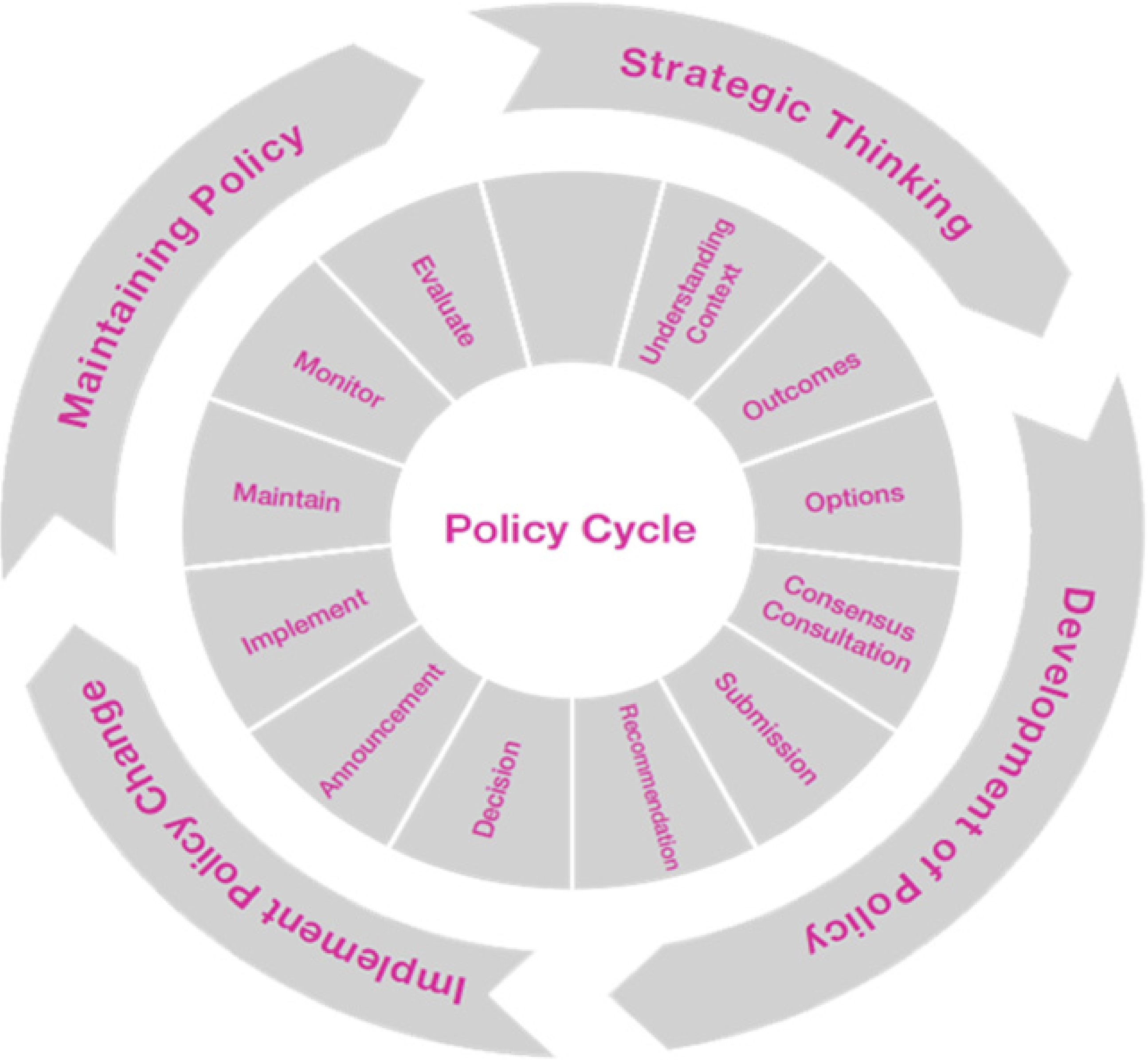
Knowledge Dissemination

- Information & Security: An International Journal, www.procon.bg/infosec
  - v.28: Critical Infrastructures Safety and Security
  - v.18: Cybercrime and Cybersecurity
  - v.15: e-Government and Security of Information
  - v. 4: Dialectics of Information Security
- Standing call:

  Cybersecurity Challenges and Responses

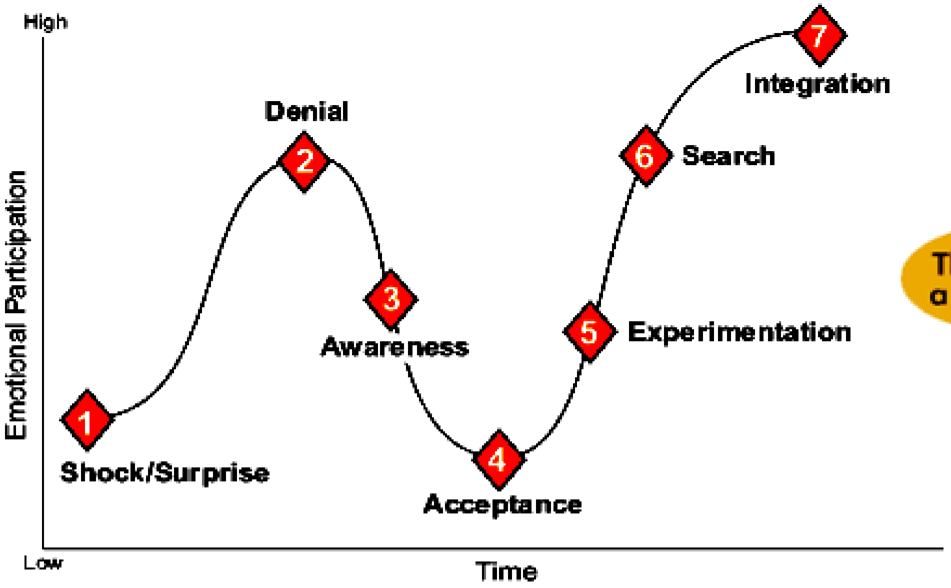
The Nowadays Cyber World

The Policy Cycle

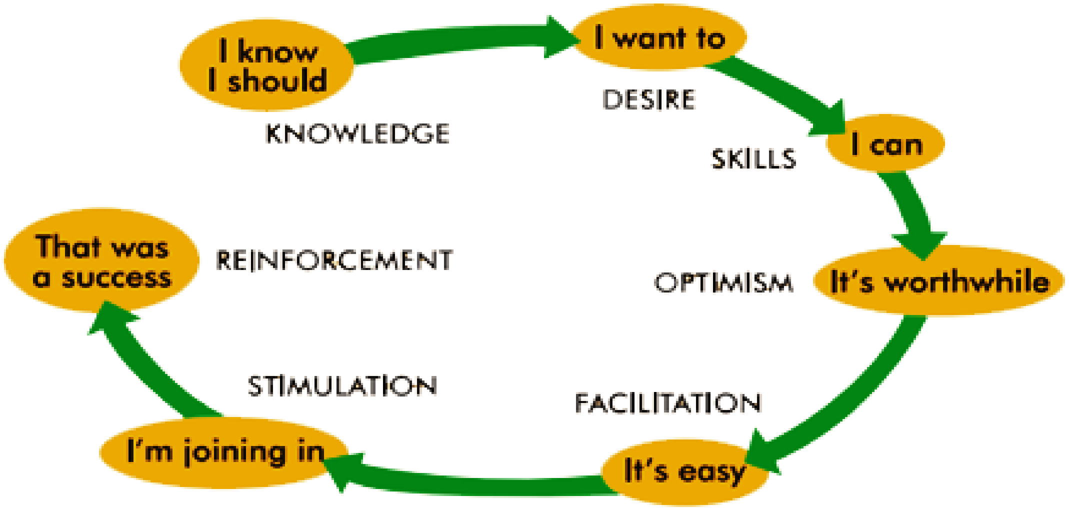


***In summary:** policy-making needs to be forward looking; outward looking; innovative, flexible and creative; evidence-based; inclusive; joined up; to learn lessons from experience; to be communicated effectively; and to incorporate ongoing evaluation and review.*

Social Awareness Rising



Change Management



Seven Steps of Social Change

Key Players

Politicians

Media

End-Users

Policy Makers

Integrated Security Sector

Cyber Experts

Civil Society

ICT Business

Other

Common Used Approaches

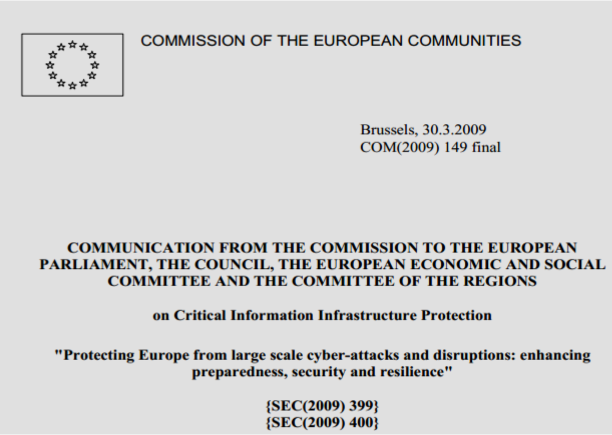
- ❑ Summits
- ❑ Sessions
- ❑ Discussions
- ❑ Forums
- ❑ Meetings
- ❑ Brainstorming & Delphi
- ❑ Surveys
- ❑ Interviews
- ❑ Media Campaigns
- ❑ Legal Acts
- ❑ Analyses
- ❑ Road Maps
- ❑ Other…

Some Examples

Recent EU Policy & Awareness Activities

enisa
European Network
and Information
Security Agency

Digital Agenda
1010111011100000100 2010-2020
for Europe



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 30.3.2009
COM(2009) 149 final

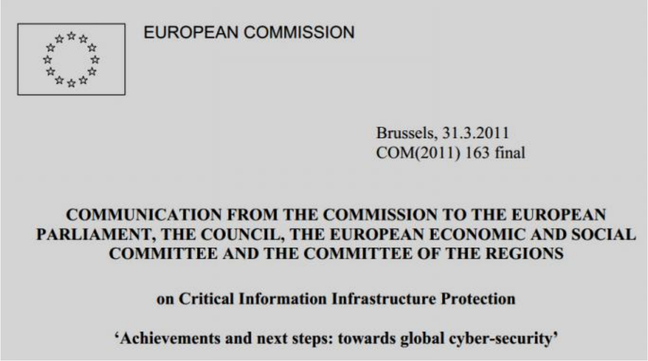
COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on Critical Information Infrastructure Protection

"Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"

{SEC(2009) 399}
{SEC(2009) 400}

Regulatory framework
for electronic communications
in the European Union



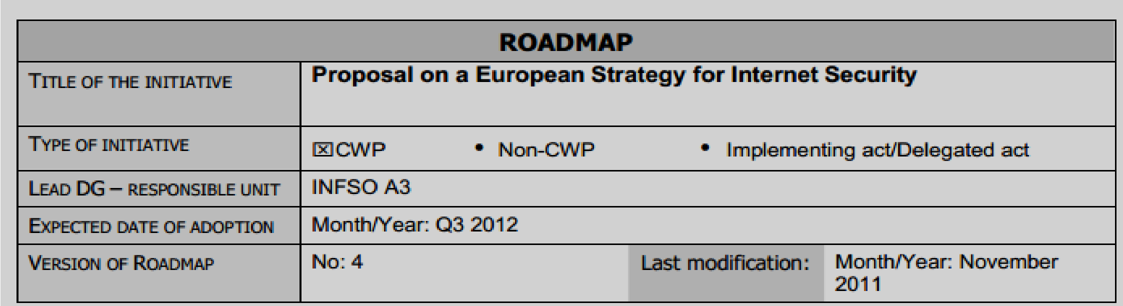
EUROPEAN COMMISSION

Brussels, 31.3.2011
COM(2011) 163 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on Critical Information Infrastructure Protection

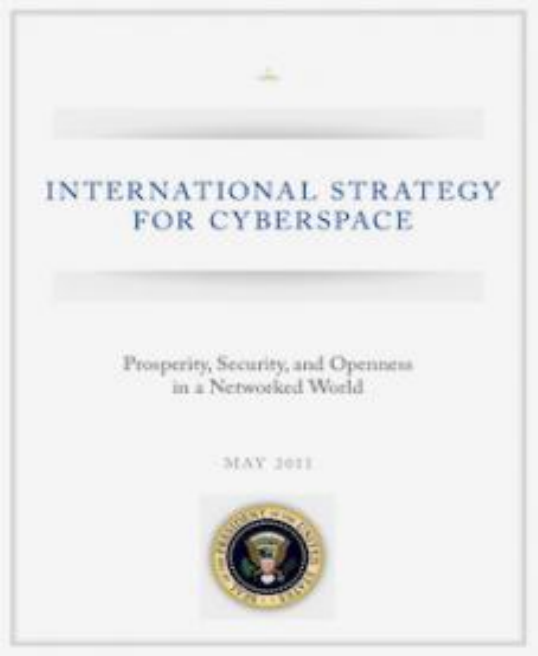
'Achievements and next steps: towards global cyber-security'



ROADMAP			
TITLE OF THE INITIATIVE	**Proposal on a European Strategy for Internet Security**		
TYPE OF INITIATIVE	☒CWP	• Non-CWP	• Implementing act/Delegated act
LEAD DG – RESPONSIBLE UNIT	INFSO A3		
EXPECTED DATE OF ADOPTION	Month/Year: Q3 2012		
VERSION OF ROADMAP	No: 4	Last modification:	Month/Year: November 2011

ACTA - Anti-counterfeiting Trade Agreement !?

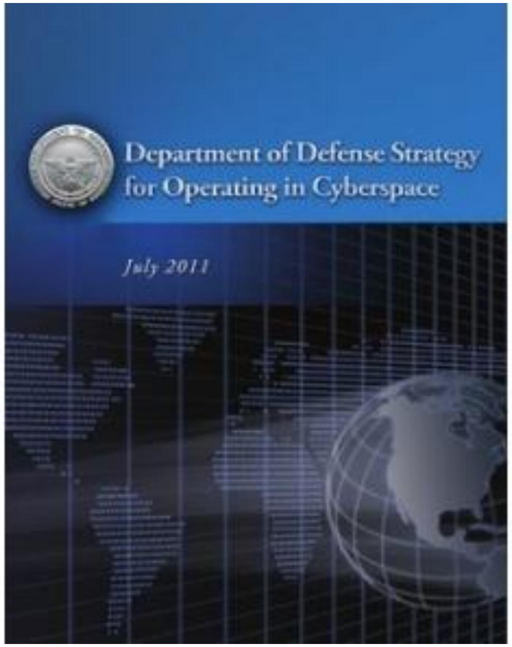
Recent USA & NATO Policy & Awareness Activities



INTERNATIONAL STRATEGY FOR CYBERSPACE

Prosperity, Security, and Openness in a Networked World

MAY 2011



Department of Defense Strategy for Operating in Cyberspace

July 2011

NATO OTAN

Defending the networks

The NATO Policy on Cyber Defence

NCIRC

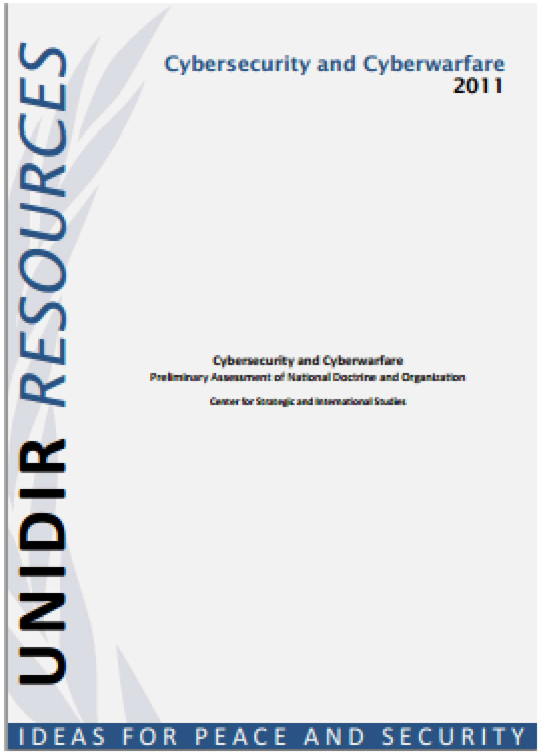
NATO COMPUTER INCIDENT RESPONSE CAPABILITY

'NATO Cyber Red Team'

'US Cyber Command'

SOPA & *PIPA* !?

Selected NGO Recent Policy & Awareness Related Activities



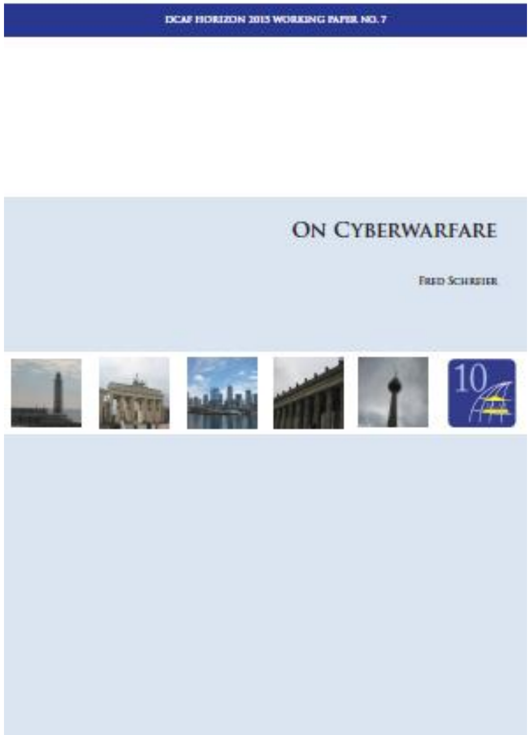
UNIDIR RESOURCES

Cybersecurity and Cyberwarfare
2011

Cybersecurity and Cyberwarfare
Preliminary Assessment of National Doctrine and Organization

Center for Strategic and International Studies

IDEAS FOR PEACE AND SECURITY



DCAF HORIZON 2015 WORKING PAPER NO. 7

ON CYBERWARFARE

FRED SCHREIER

10

Scoop.it!

CYBER STRATEGY
Protect, Defend, Attack

Institute of ICT
Bulgarian Academy Of Sciences

BULGARIAN
ACADEMY
of SCIENCES
1869

IICT

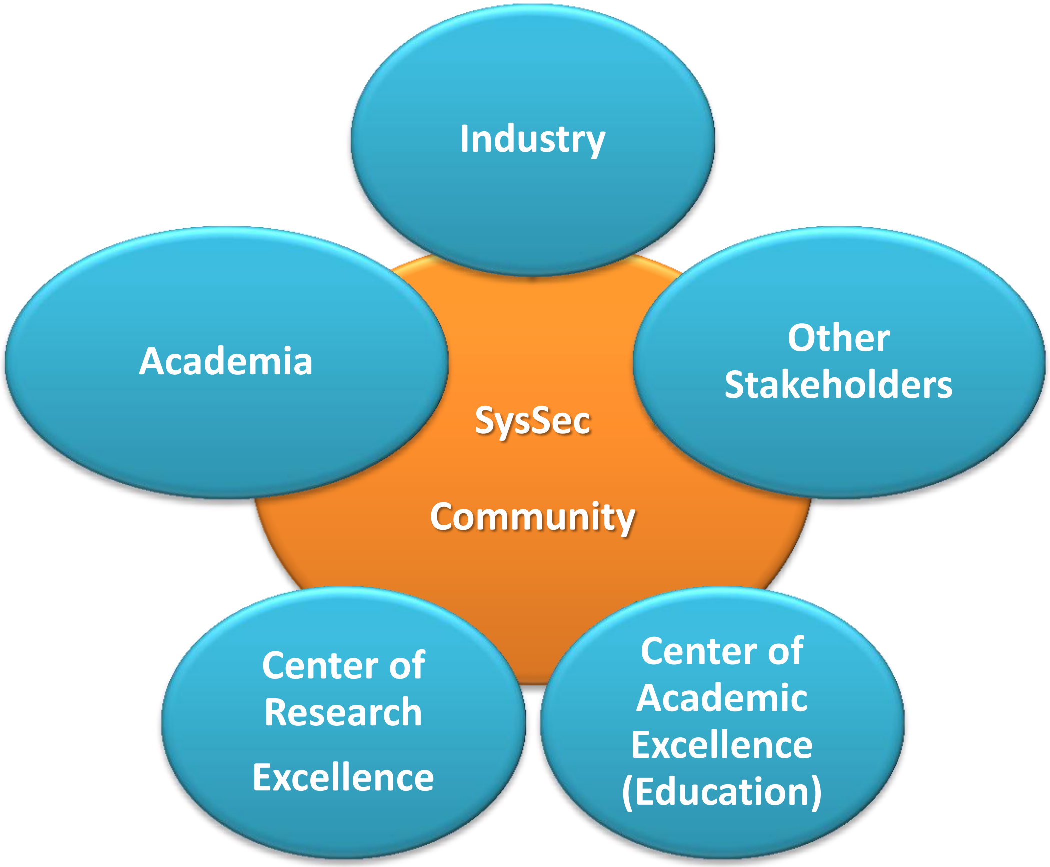
IT for Security Department

http://it4sec.org

Computer Networks & Architectures Department

http://www.acad.bg/rismim/en/indexen.htm

A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World, SySSec, EU FP7

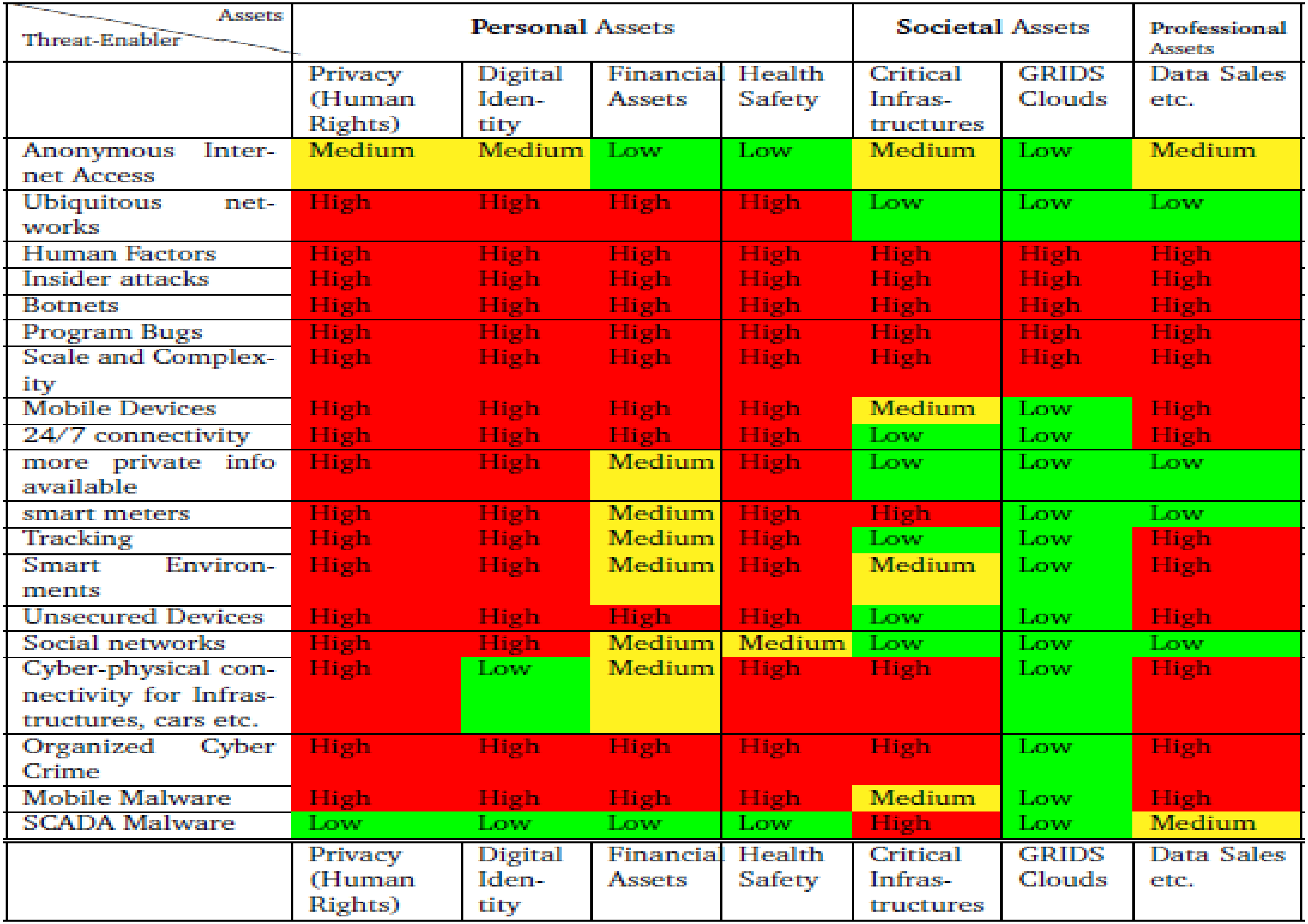

Industry
Academia
Other Stakeholders
SysSec
Community
Center of Research Excellence
Center of Academic Excellence (Education)

... Instead of reactively chasing after attackers, we should start working proactively and think about emerging threats and vulnerabilities...

syssec

http://www.syssec-project.eu

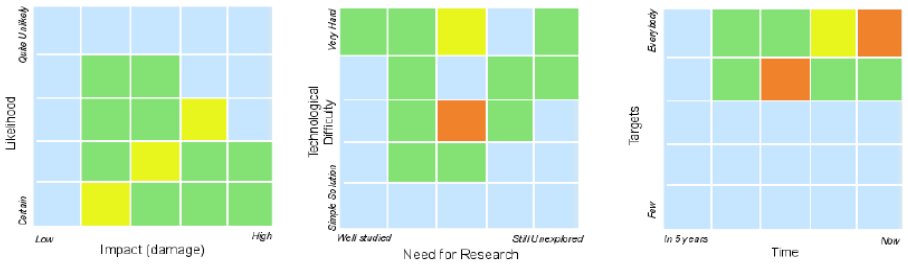
SySSec Cybersecurity Priorities 2011



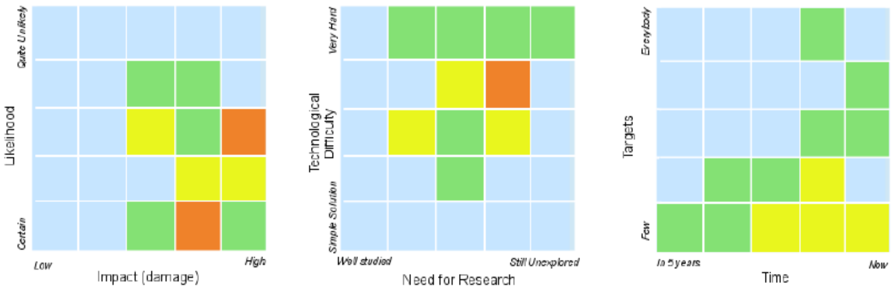
Assets Threat-Enabler	Personal Assets				Societal Assets		Professional Assets
	Privacy (Human Rights)	Digital Identity	Financial Assets	Health Safety	Critical Infrastructures	GRIDS Clouds	Data Sales etc.
Anonymous Internet Access	Medium	Medium	Low	Low	Medium	Low	Medium
Ubiquitous networks	High	High	High	High	Low	Low	Low
Human Factors	High	High	High	High	High	High	High
Insider attacks	High	High	High	High	High	High	High
Botnets	High	High	High	High	High	High	High
Program Bugs	High	High	High	High	High	High	High
Scale and Complexity	High	High	High	High	High	High	High
Mobile Devices	High	High	High	High	Medium	Low	High
24/7 connectivity	High	High	High	High	Low	Low	High
more private info available	High	High	Medium	High	Low	Low	Low
smart meters	High	High	Medium	High	High	Low	Low
Tracking	High	High	Medium	High	Low	Low	High
Smart Environments	High	High	Medium	High	Medium	Low	High
Unsecured Devices	High	High	High	High	Low	Low	High
Social networks	High	High	Medium	Medium	Low	Low	Low
Cyber-physical connectivity for Infrastructures, cars etc.	High	Low	Medium	High	High	Low	High
Organized Cyber Crime	High	High	High	High	High	Low	High
Mobile Malware	High	High	High	High	Medium	Low	High
SCADA Malware	Low	Low	Low	Low	High	Low	Medium
	Privacy (Human Rights)	Digital Identity	Financial Assets	Health Safety	Critical Infrastructures	GRIDS Clouds	Data Sales etc.

2012 Roadmap Update

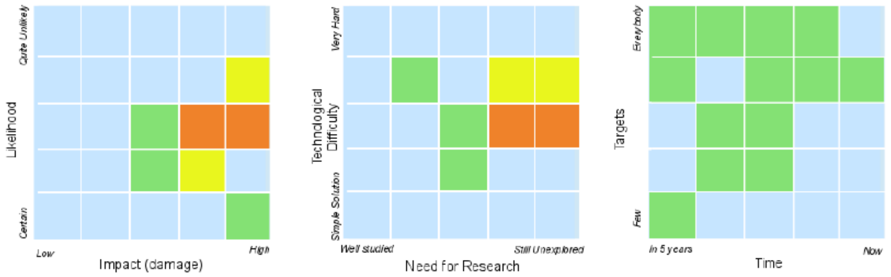
System Security Aspects of Privacy



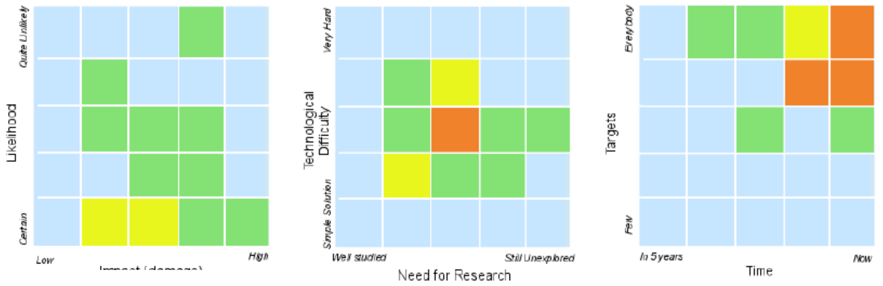
Collection, Detection, and Prevention of Targeted Attacks



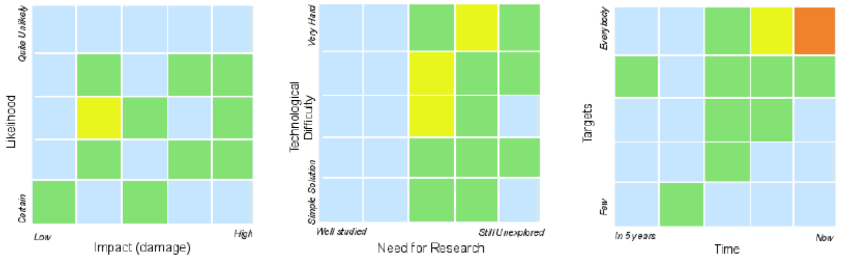
Security of New and Emerging Technologies

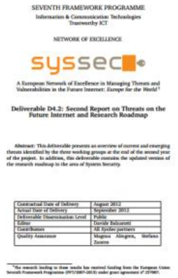


Security of Mobile Devices



Usable Security





SEVENTH FRAMEWORK PROGRAMME
Information & Communication Technologies
Trustworthy ICT

NETWORK OF EXCELLENCE

syssec

A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: *Europe for the World*[1]

Deliverable D4.2: Second Report on Threats on the Future Internet and Research Roadmap

Abstract: This deliverable presents an overview of current and emerging threats identified by the three working groups at the end of the second year of the project. In addition, this deliverable contains the updated version of the research roadmap in the area of Systems Security.

Contractual Date of Delivery	August 2012
Actual Date of Delivery	September 2012
Deliverable Dissemination Level	Public
Editor	Davide Balzarotti
Contributors	All SysSec partners
Quality Assurance	Magnus Almgren, Stefano Zanero

[1] The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257007.

A Study on IT Threats and Users Behavior Dynamics in Online Social Networks, DMU03/22, 2011-2013

IICT

NATIONAL
SCIENCE
FUND

SEVENTH FRAMEWORK PROGRAMME

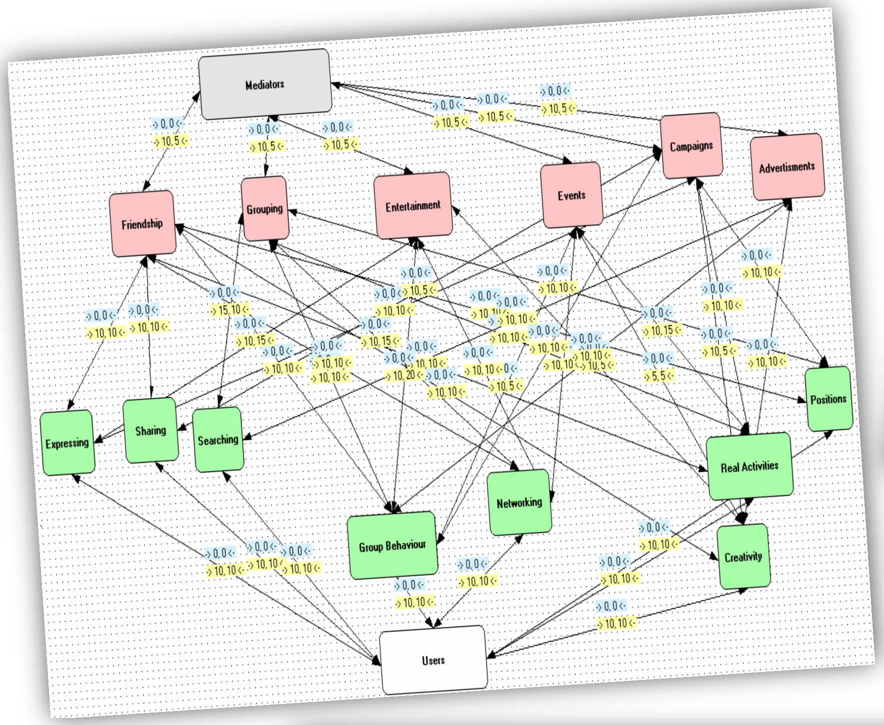
syssec

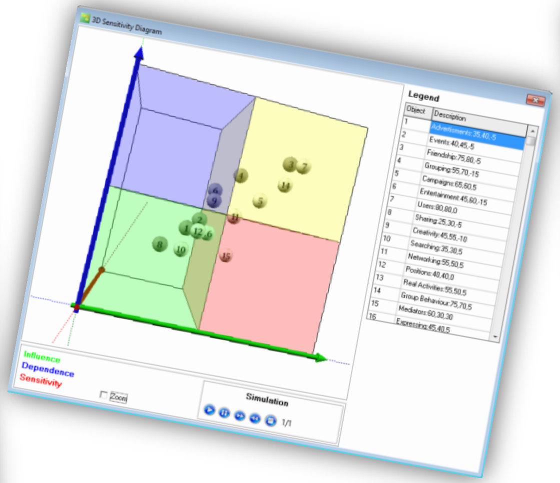
www.snfactor.com

www.syssec-project.eu

Some of our activities in 2012

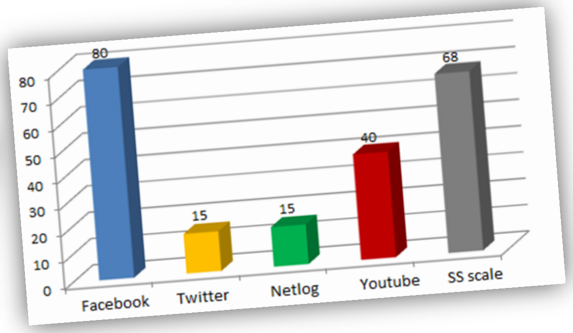
Recent Results





Legend

Object	Description
1	Advertisments:35,40,-5
2	Events:40,45,-5
3	Friendship:75,80,-5
4	Grouping:55,70,-15
5	Campaigns:65,60,5
6	Entertainment:45,60,-15
7	Users:80,80,0
8	Sharing:25,30,-5
9	Creativity:45,55,-10
10	Searching:35,30,5
11	Networking:55,50,5
12	Positions:40,40,0
13	Real Activities:55,50,5
14	Group Behaviour:75,70,5
15	Mediators:60,30,30
16	Expressing:45,40,5

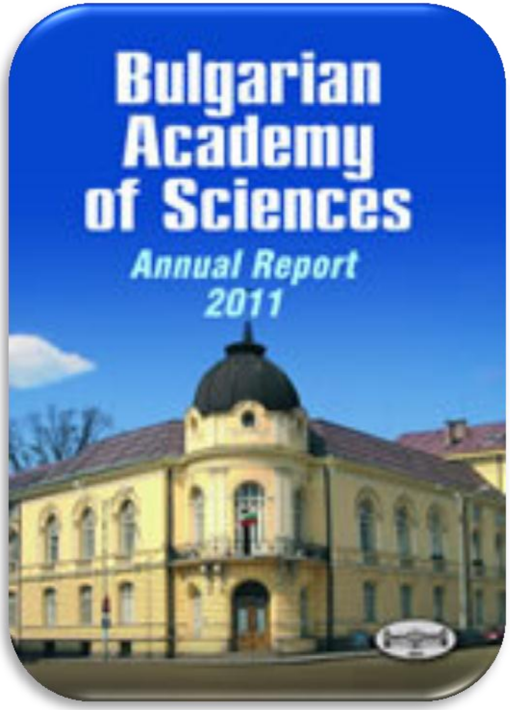


BULGARIAN
ACADEMY
of SCIENCES
1869

National Laboratory of Computer Virology

http://www.bas.bg/cgi-bin/e-cms/vis/vis.pl?s=001&p=0317&n=4&g=

Recent Results: New Methods for malware attacks prevention with applications for contents recognition in real-time for multicore configuration and cloud computing (Team Leader Prof. Eugene Nikolov)



Institute of Mathematics & Informatics

Mathematical Foundations of Informatics Department

RESEARCH FIELDS: Coding theory, Cryptography, Combinatorics, Theorethical informatics

Institute of Defence - MoD

ИНСТИТУТ ПО ОТБРАНА

http://www.mod.bg/bg/EXT/InstitutOtbrana/index.htm

HEMUS 2012

DEFENCE, ANTITERRORISM AND SECURITY

Sixth International Conference

Smart Defence
Solutions and Technologies

31st May - 1st June 2012, Plovdiv, Bulgaria

UNDER THE AUSPICES OF

MINISTRY OF DEFENCE
OF THE REPUBLIC OF BULGARIA

MINISTRY OF ECONOMY, ENERGY
AND TOURISM
OF THE REPUBLIC OF BULGARIA

GENERAL PARTNERS

IFP
International Fair Plovdiv

Bulgarian Defence
Industries Association

ORGANIZERS

Defence Institute

HEMUS
HEMUS-95 Foundation

http://di.mod.bg/hemus2012/

Thematic areas:

Armaments & combat supplies
Combat equipment & systems
CBRN protection and ecology
Combat supply
Communication and Information Systems & Technologies
Radiolocation & navigation
Informatics & Information Technologies
Cyberdefence, cryptography & Information Security
Defence Economic Aspects
Logistics
Military-political studies
Human Factor & Medicine
Military Standards, quality and specifications
Military Tests & Control Measurements

National Military University

Artillery, AAD & CIS Faculty
http://www.nvu.bg/node/361

Shumen, November 3-4, 2011

http://www.aadcf.nvu.bg/science/new.2011.html

Scientific Session 2011

Problems of Information Security of XXI century Proceedings

University of Library Research & Information Technologies

БИТ
УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ
STATE UNIVER
LIBRARY STUDIES AND INFORMATION TECHNOLOGIES

Scientific-Research Lab for Cybersecurity

Leader: Prof. Dragomir Pargov

International Conference 'Bulgarian Cryptography Days' BulCrypt 2012

ФОНД
НАУЧНИ
ИЗСЛЕДВАНИЯ
Министерство на образованието, младежта и науката

Sofia University “St. Kliment Ohridski”

Partner on the International Cyber Investigation Training Academy

Sofia University – Center for Educational Services

Cybersecurity - one year qualification course

DISCUSSION

The policy making and awareness rising processes concerning the human society are rather complex research field. Whilst, nowadays the cybersecurity is an indispensible part of the 21st century information society the solution of this task is evidently becoming a serious challenge that incorporates a comprehensive necessity for integration of academic research in both social and technical sciences.

THANK YOU FOR THE ATTENTION!

QUESTIONS?