



The Estonia cyber attacks of 2007

>> PROFESSOR PEETER LORENTS

Head of the R&D Branch
the NATO Co-operative Cyber Defence Centre of Excellence
Tallinn, Estonia





CCDCOE

Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

Cyber Society, Cyber Security
Problems, Solutions and Developments
NATO CCD COE



Agenda

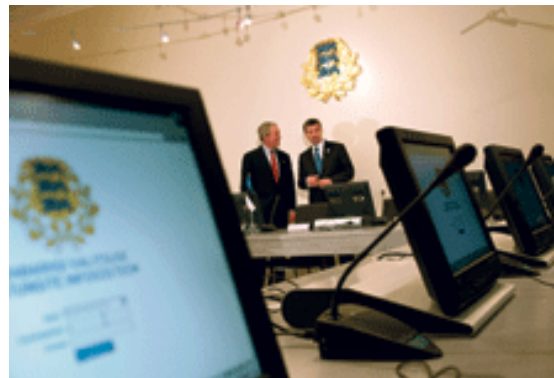
- **Cyber Society – Estonian Way**
- **Why Cyber Defense?**
- **Cyber Attacks Against Estonia
in the Spring of 2007**
- **Estonian Actions**
- **Lessons Learned**
- **NATO CCD COE**



Cyber Society – Estonian Way

- National ID card for identification and digital signature
- Payment and identification via cell phone
- Critical services provided via Internet

- E-banking
- E-tax board
- E-school
- E-court
- E-police
- E-health



- The Estonian Government works as e-cabinet
- First online parliamentary elections in the world



Estonian Public Sector Depends on the Cyberspace

- National ID card for identification and digital signature:
more than 1 million ID-cards issued
- Critical public services provided via Internet e-tax board:
over 80% usage
- Commercial registry:
over 25% usage
- State Gazette:
100%
- X-road as the gateway **for all public databases**



Why Cyber Defense?

Attacks in Cyberspace is a Threat to Everyone

Estonian Case:

- Bronze Soldier riots in April 2007 and **cyber attacks**
- Defacement attacks, spam campaign and botnet attacks
- Targeted against Estonian parliament, government, internet service providers and online services as banking and media
- Estonia was able to survive due to the secure network infrastructure and a good cooperation within and between public and private sector





Cyber Attacks against Estonia. Main targets

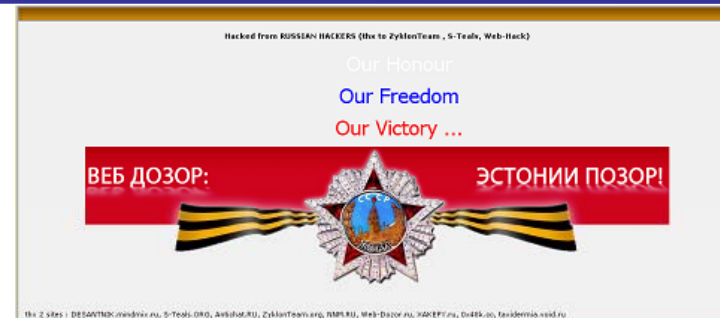
- **Political targets**
Government, parliament, ministries, police etc.
- **Services**
Banks, internet providers, media
- **Network infrastructure**
Routers and DNS servers
- **Other targets**
Small companies, schools, ...ee



Cyber Attacks against Estonia.

Nature of the Attack

- DoS attacks, some DDoS
- Defacement attacks
 - E-mail and comment spam
 - Targets: government web sites, news portals
- Calls to attack Estonia in the Internet:



Сегодня, проводится грандиозная DoS-атака на сайт их правительства <http://www.riik.ee/et/>
 ооуществить это легко - заходим в Пуск - Стандартные -
 командная строка, в открывшемся окне пишем :
ping -n 5000 -l 1000 http://www.riik.ee
 на это вы потратите 5 мегабайт исходящего трафика.



Cyber Attacks against Estonia.

Main attack phase

Testing the defenses (30APR-03MAY07)

- Use of botnets (DDoS)
- Targeted attacks against network infrastructure (routers and DNS servers)

Testing for bandwidth ceiling

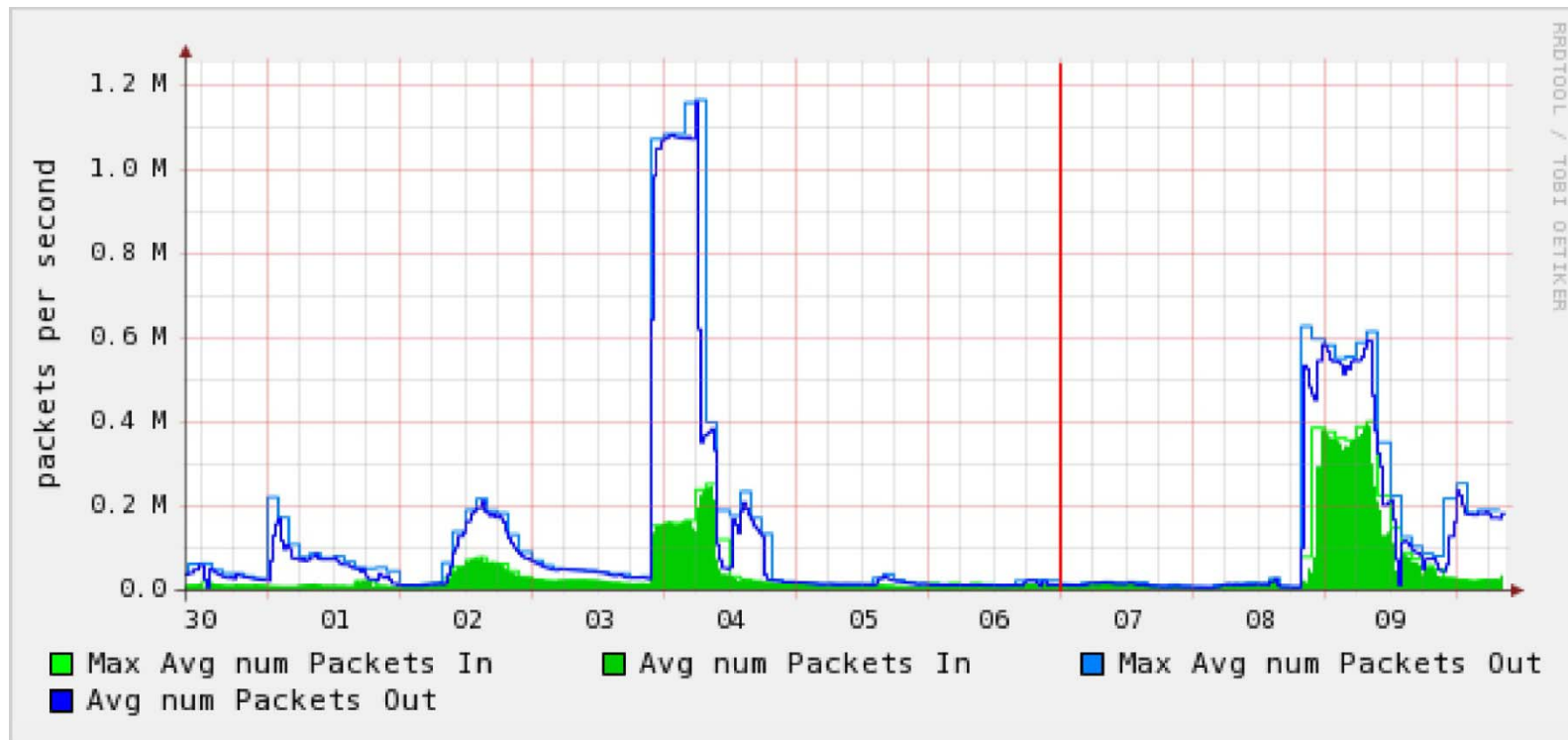
84.50.56.251 tuvasta.politsei.ee - [30/Apr/2007:16:53:48+0300]

"GET/failid/s_ansip1..jpg?id=2126121&ANSIP_PIDOR=FASCIST
HTTP/1.1" 404 345 "-" "ch"



Cyber Attacks against Estonia.

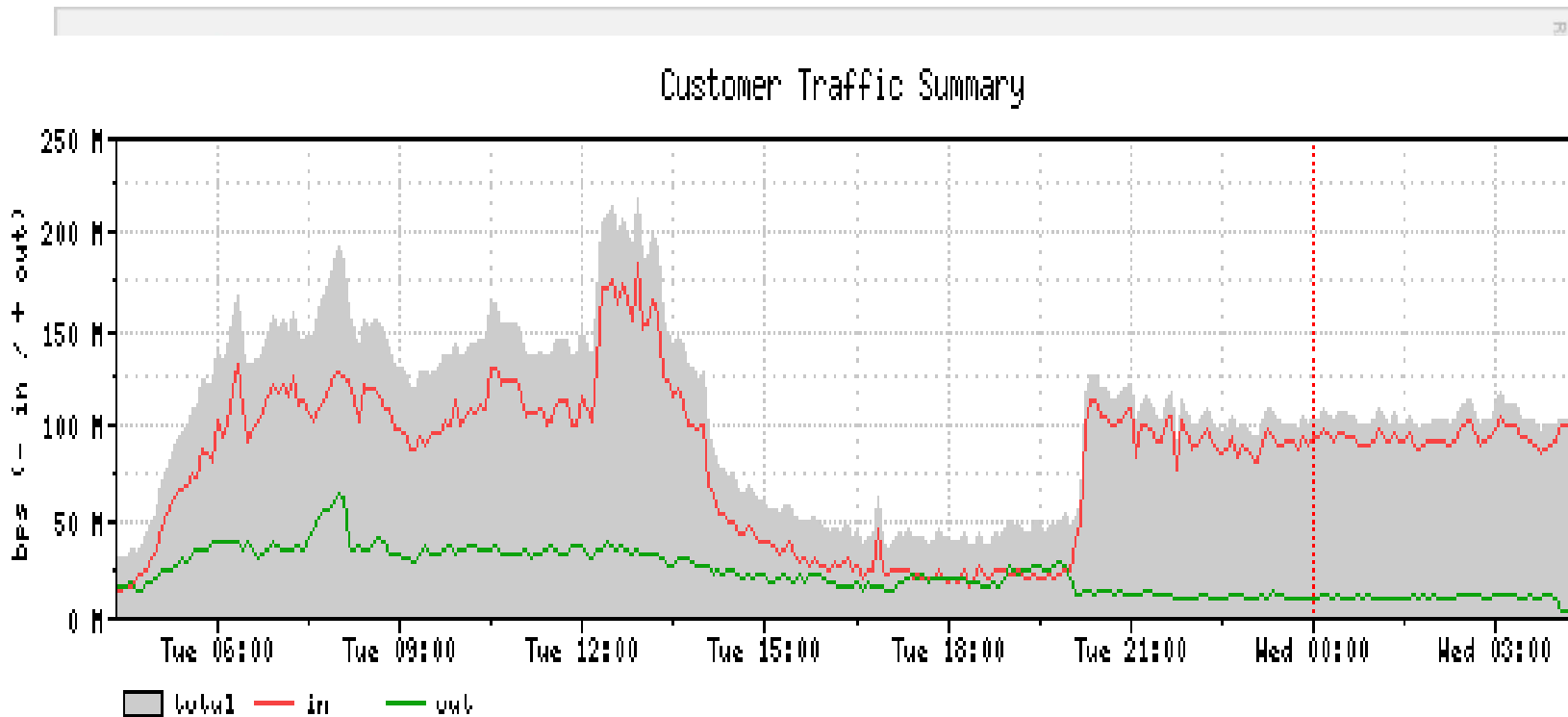
Largest DDoS attack on 04MAY07





Cyber Attacks against Estonia.

DDoS starting 2000 GMT 08MAY07



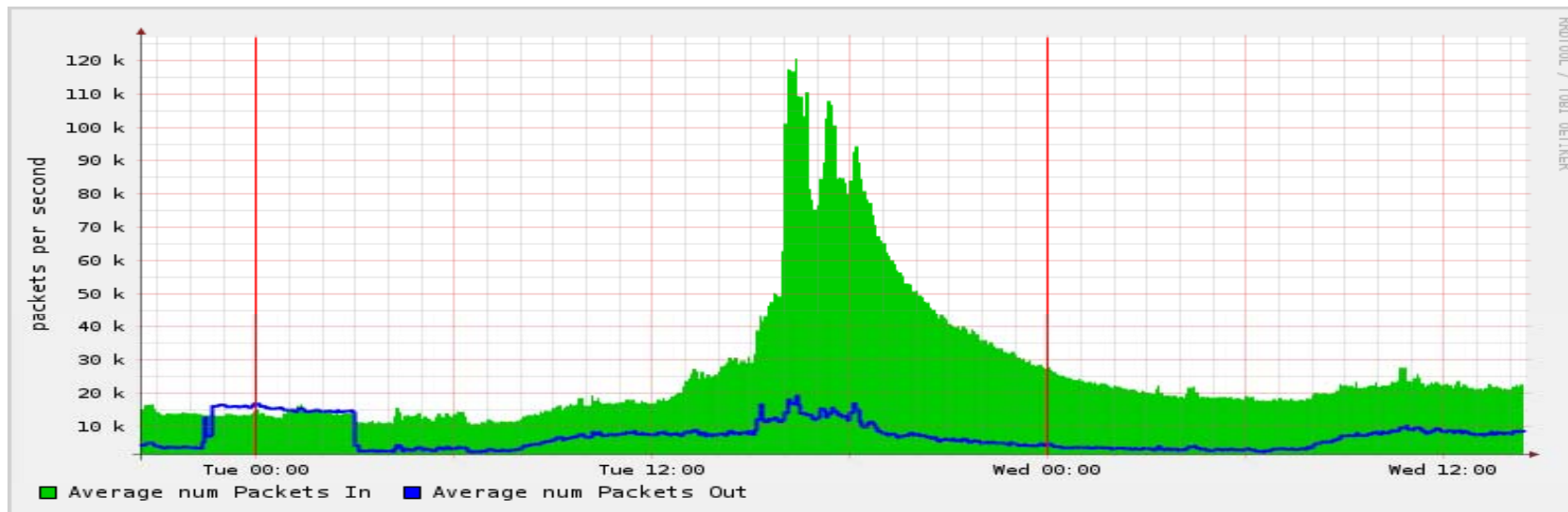
Professor Peeter Lorents, CCD COE Chief of the R&D Branch



Cyber Attacks against Estonia. DDoS against banks

10MAY07 Hansabank
15MAY07 SEB Eesti Ühispank
+ various attacks against smaller banks

15MAY07 – large DDoS against govt. sites.





Cyber Attacks against Estonia. Follow-on phase

- Short DDoS on 18MAY07



Cyber Attacks against Estonia. Defensive Actions

- **Cooperation and coordination**
between the public and private sector with nations and international organizations
- **Network configuration**
filtering
increasing bandwidth
blocking access
white-listing
- **Information sharing and media coverage.**



Lessons Learned from the Estonian Case

Importance of Internal Cooperation

- Network of leaders and specialists
- Public and private sector cooperation
- Proactive defence

Importance of International Cooperation

- Political
- Technical
- Legal etc.



Estonian Initiative: Cooperative Cyber Defence Centre of Excellence

- **Cooperation** is key for effective defence
- There are **no physical borders** in the cyberspace
- The **cyberspace has to be protected** like air, sea or land
- **Defence is a sum** of political, legal, technical ... measures



Cyber Defense Issues for NATO

Cyberspace is not always secure

- Unauthorized Intrusions
- Hostile Scanning
- Defacements
- Propaganda
- Domain Name Server Attacks
- Distributed Denial of Service (botnet) Attacks
- Computer Viruses
- Compound Attacks



Problem areas for NATO

- How to define and fight common threats in the cyberspace?
- How is network security related to (inter)national security?
- Where to draw the line between cyber crime, cyber terrorism and cyber war?
- What of the above should be the concern for the Cyber Defence Capability?



Cooperative Cyber Defence Centre of Excellence CCD COE

Mission and Vision



Mission: to enhance the cooperative cyber defence capability of NATO.

Vision: to become a primary source of expertise for NATO in cooperative cyber defence-related matters.



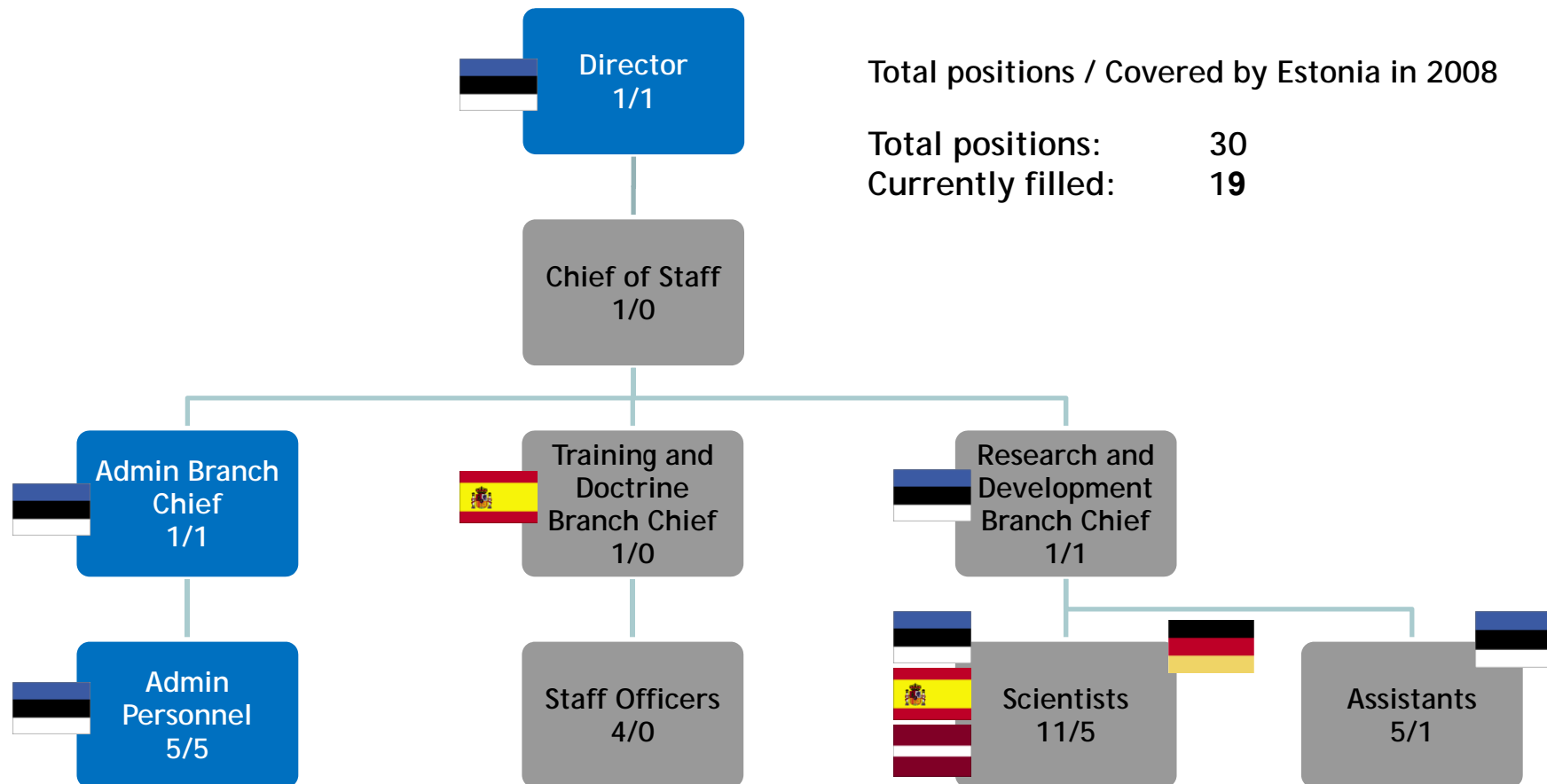
Main Functions

- Input to doctrine and concepts in the field of cyber defence
- Cyber defence related analysis, education, awareness and training
- Research and development projects in the field of cyber defence
- Cyber defence related analysis and lessons learned





Organization





Status

IMO – International Military Organization

- **NATO Accreditation (28.10.2008.)**
- **MoU (14.05.2008.)**



Relationships



NATO entities

- HQ SACT
- NATO CDMA
- NCIRC
- NC3A

Other entities

- Universities
- Private sector

Customers

- NATO
- Sponsoring Nations
- Contributing Participants

NATO COE-s

- COE-DAT
- C2 COE

Nations

- NATO
- Non-NATO



NATO Projects

2007

1. Input to the NATO Cyber Threat Assessment
2. Input to the NATO Cyber Defense Concept
3. Input to the NATO Computer Security Course
4. Participation in NATO Cyber Defense Events

2008

1. Support of NATO Cyber Defense Exercise
2. Implementation of NATO Cyber Defense Concept
3. Cyber Defense Legal Aspects
4. Cyber Security Doctrine and Strategy
5. Security Methodologies
6. Cyber Defense Lessons Learned



NATO projects (Proposals)

2009

1. Provide advice on the repercussions of international incidents and how to respond
2. Provide advice for the NATO Cyber Defense Infrastructure establishment
3. Support EX STEADFAST JOIST 09
4. Support EX STEADFAST JUNCTURE 09
5. Examine Cyber Defense in the NNEC Environment
6. NATO Cyber Defense Concept v2.0
7. Concept of Cyber Warfare
8. Legal Aspects of Cyber Defense
9. Legal Training for NATO Lawyers in the area of IT and International Law
10. Computer Security Incident Response Team Interoperability Standards



NATO projects (Proposals cont.)

2009

- | | |
|-----|---|
| 11. | Hands on Training Development |
| 12. | Development of Cyber Lab |
| 13. | Development and Execution of Cyber Defense Exercise |
| 14. | Development of Penetration Team |
| 15. | Publish Cyber Defense Lessons Learned |
| 16. | Cyber Security Doctrine/ Strategy |
| 17. | Security Methodologies |



Value and benefit

For NATO:

- Cyber defense capability
- Source of expertise

For Sponsoring Nations:

- Information and knowledge
- Network of specialists
- Free admission to the courses

Sponsoring Nations
October 2008

