Egils Stūrmanis
DDIRV manager
State Joint Stock Company
“State Information Network Agency”

2008.09.26 Vienna 25th TF-CSIRT Meeting
Baltic states - Latvia

- Capital – Riga,
- Population - 2,27milj,
- Territory 64,589 km²,
- EU from 01.05.2004,
- NATO from 29.03.2004,
- Internet use % of population:
  - 6% (2001)
  - 22% (2004)
  - 36% (2005)
  - 43% (2006)
  - 54% (2007)
  - 63% (2008)

Source: http://www.eps.gov.lv/index.php?&701
Establishing of DDIRV

- Government decision on April 2005 to support establishing National Computer security incident response team,
- End of 2006 funding was provided to Ministry of Transport,
- Ministry of Transport delegate CSIRT functions to JSC “State Information Network Agency”,
Constituency

- Governmental authorities,
- Municipalities,
- State Network Information agency business customers,
- More than 700 “State private electronic communication network” connections around all country, most of them are internet customers too,
- Around 50k end-users, into AS8194.
Staff & Resources

- Team manager,
- IT security engineer.

- RTIR incident tracking system,
- Webpage [www.ddirv.lv](http://www.ddirv.lv),
  - Web form to report incident (SSL)
  - Web form to registration in constituency (SSL)
- IDS/IPS network monitoring,
- Honeypot with EURECOM. [https://riviera.eurecom.fr/](https://riviera.eurecom.fr/)
Services

- Incident handling,
- Newest vulnerabilities and viruses publishing on webpage, (available RSS)
- Providing consultations and recommendations,
- Publishing incident statistics,
- DDIRV don’t offer commercial services,
- The DDIRV hours of operation are restricted to regular business hours.
International cooperation

- DDIRV is delegated as an expert of ENISA's National Liaison Officer of Latvia,
- Trusted introducer – to achieve accredited status just now,
- Membership in FIRST – next future,
- Closest contacts with Baltic states CERT’s, Europe and worldwide.
Domestic cooperation

- Latvia CERT team working group [http://www.cert.lv/](http://www.cert.lv/)
Threats - past and future

- Estonia - cyberwar spring 2007,
- Lithuania - massive webpages defacing may 2008,
- Georgia – limited access to domain *.ge after midle of July 2008,
- Latvia – question is not “to be or not to be”, but when and how.
Announcement

Operation of SEB Eesti Ühispank’s internet services is temporarily disturbed.

We are currently experiencing distributed denial of service attack which is causing overload in our online systems. Therefore access to our internet services is blocked outside Estonia. Please note that e-mails from servers located outside Estonia might not be delivered to recipients in the bank.

Card payments, ATMs, self service terminals, telephone banking and branch offices are working as usual and customers' financial information is not in threat.

We would like to apologise for your inconvenience and we hope to return to our normal operations of online services as soon as possible.
Вы бъёдё все с ума посходили, считаете себя благороднейшей нашней?
Благородные люди делают все что могут для своей страны, а не уничтожают ее как вы. Так ладно бъёдё, ваша участь понятна - зло, и как следствие неудачна, но бъёдё вы же еще больше наплодите таких же уродов, закомплексованных ублюдков.
Before the Gunfire, Cyberattacks

By JAMES BARRON
Published August 13, 2008

Weeks before bombs started falling on Georgia, a security researcher in suburban Massachusetts was watching an attack against the country in cyberspace.

Jose Nazario of Arbor Networks in Lexington noticed a stream of data destined for Georgian government sites containing the message: "with love for Russia."

Other Internet experts in the United States said the attacks against Georgia's Internet infrastructure began as early as July 20, with coordinated barrages of millions of requests — known as distributed denial of service, or D.D.O.S. — attacks that overloaded and effectively shut down Georgian servers.

Latvia, July 2008
Conclusions

- has an infrastructure and resources possible work in crisis situation,
- have to get lessons from Estonia and Lithuania,
- have to improve international contacts,
- cooperation and coordinated activities are key for success.
Thanks!

DDIRV
Kr. Valdemara street 110
Riga, LV1013, Latvia
Phone: 67029583,
E-mail: info@ddirv.lv
Webpage: http://www.ddirv.lv