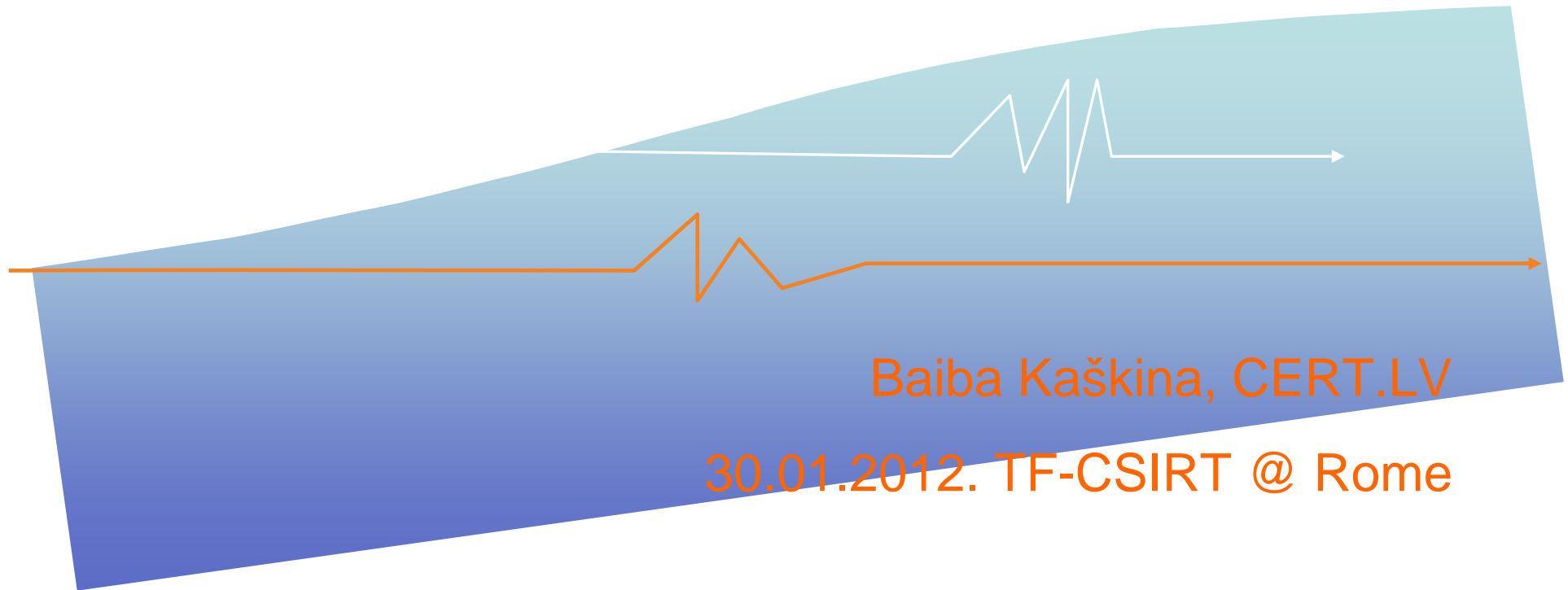


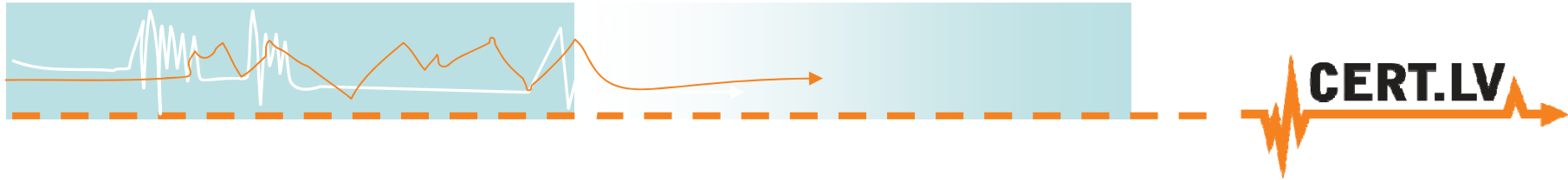


Spamhaus issues



Baiba Kaškina, CERT.LV

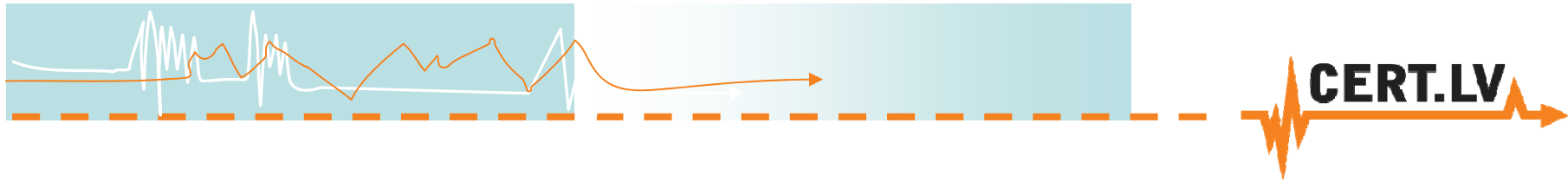
30.01.2012. TF-CSIRT @ Rome



Spamhaus story - history

- Conflict in 2010., open letter on CERT NIC.LV vs. Spamhaus
- Discussions @ TF-CSIRT
- Action item: “31.1. TI Review Board to discuss how to deal with Spamhaus problems and what further action to take” – awaiting information from CERT.LV
- Email to TF-CSIRT with example (June 2011)
 - No feedback

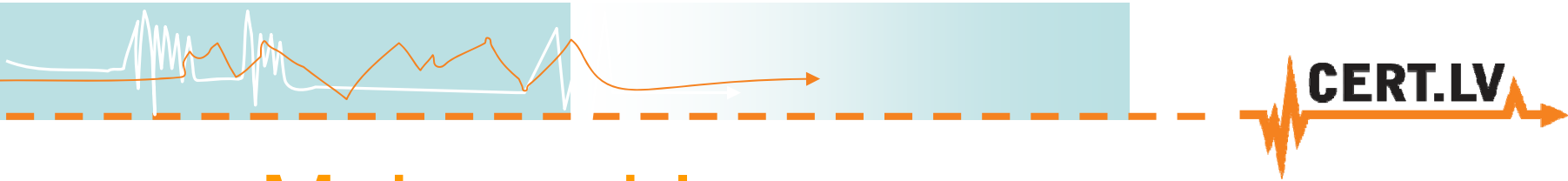




Spamhaus – situation in Latvia

- Data centres are interesting for customers from Russia, Ukraine, Belarus, etc.
- Several serious blacklistings in 2011
 - Lattelecom blacklisted since 7 January 2012
- ISPs are willing to cooperate, Spamhaus not

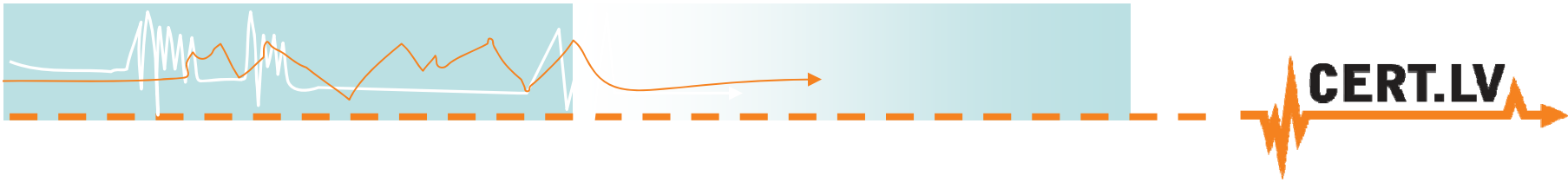




Main problems

- Information Spamhaus provides is not sufficient to file an incident report
- Blacklisting based on outdated information
- Spamhouse is very slow on answering, providing additional information on why the IP is blacklisted
- Escalation errors and exaggerations
- Escalation procedure is nowhere documented – how far it can go?
- Very slow reaction on removal from blacklists
- Spamhaus is not cooperating even with those who are responding, including CSIRTs
- Blacklisting transit providers – is it really a correct approach?

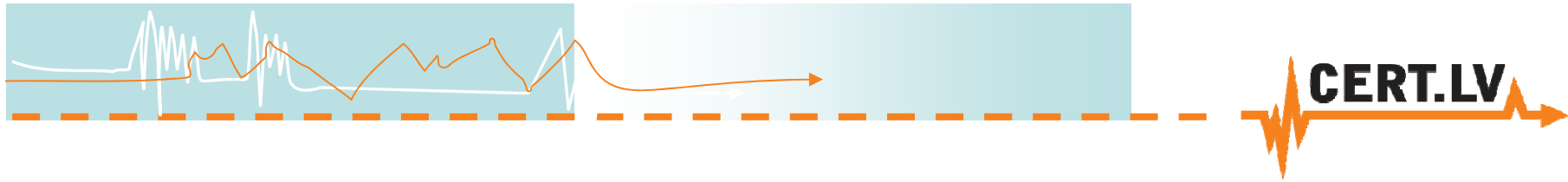




Decision?

Do we as CSIRTs and ISPs
have problems with Spmahaus
or not?

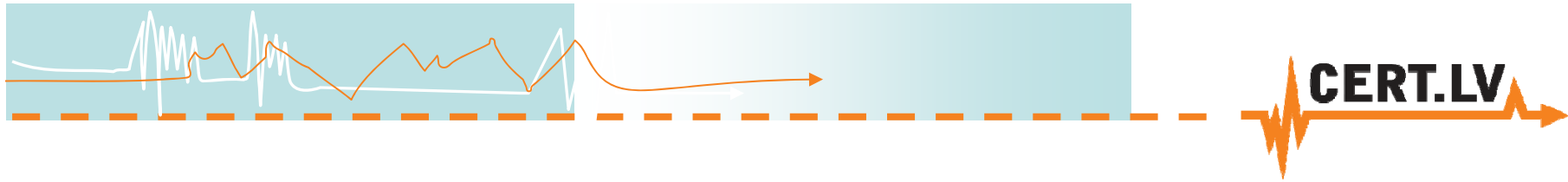




Yes?

- We should do something to prevent Spamhaus from spending our time and resources
- There should be somebody - an authority who could control and supervise Spamhaus activities





Thank you!!!

<http://www.cert.lv/>
cert@cert.lv
baiba.kaskina@cert.lv

