

# DDoS and the cloud

**Giovane C. M. Moura**

`giovane.moura@sidn.nl`

`https://sidnlabs.nl`

**Panel: On the Cyber Dimension  
of Enterprise Cloud Management**

IFIP/IEEE IM 2017

May 10th, 2017

Lisbon, Portugal

# The cloud

- ▶ Is just somebody else's computer (to quote Schneier)
- ▶ Advantages: costs and simplicity
  - ▶ shared costs → shared risks
- ▶ Disadvantages: trust
- ▶ It works pretty well until...

# DDoS on a cloud

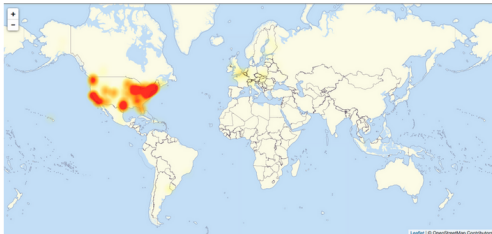


The New York Times

TECHNOLOGY

## *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*

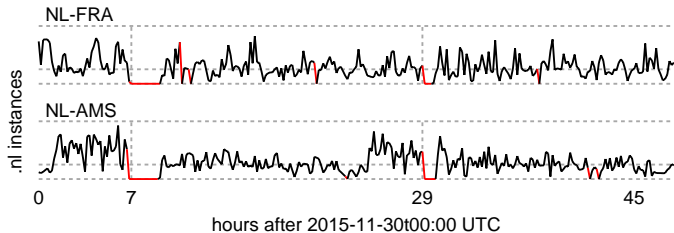
By NICOLE PERLROTH OCT. 21, 2016



- ▶ Dyn, a DNS provider, was attacked
- ▶ Netflix, Spotify, NY Times, Airbnb all affected

# DDoS on a cloud

- ▶ Cloud has tons of virtualization
- ▶ But most of time, a shared pipe
- ▶ Collateral is a big thing: ProtonMail, Dyn, etc.
- ▶ You're also sharing risks<sup>1</sup>.



**Figure:** Normalized number of queries for `.nl`, measured at the servers in 10 minutes bin, during DDoS on the Root DNS – red shows collateral damage

<sup>1</sup>Giovane C. M. Moura, Ricardo de O. Schmidt, John Heidemann, Wouter B. de Vries, Moritz Müller, Lan Wei and Cristian Hesselman. Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event. ACM IMC2016