Like vuls in rain

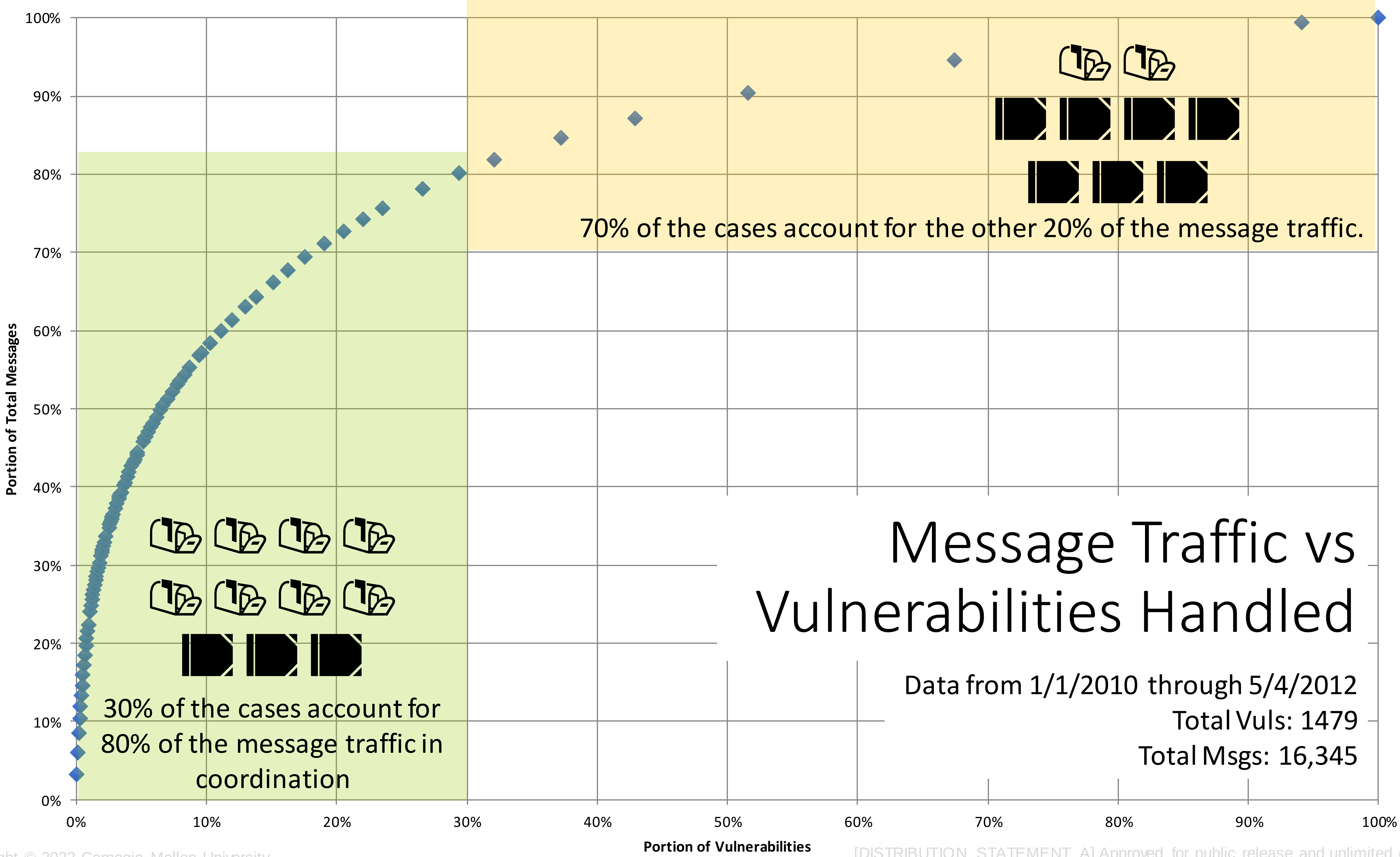
Allen Householder
CERT/CC
@__adh__

Coordinated Vulnerability Disclosure (CVD) at CERT/CC

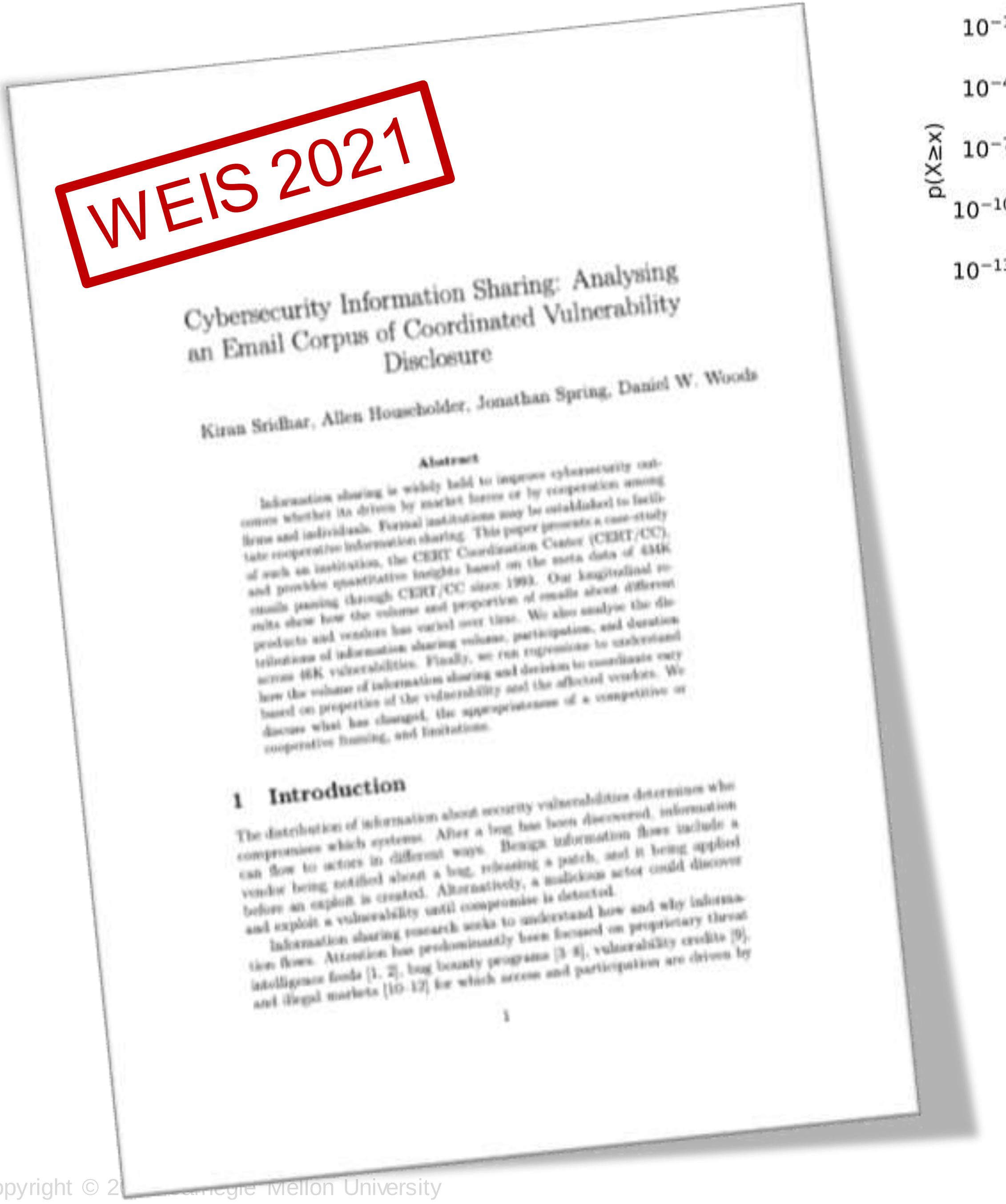
Email data set spans 1993-2020

- 434k messages
- 46k vulnerability cases
- 250 vendors

(+)/ ?



Message Traffic vs Vulnerabilities Handled
Data from 1/1/2010 through 5/4/2012
Total Vuls: 1479
Total Msgs: 16,345
70% of the cases account for the other 20% of the message traffic.
30% of the cases account for 80% of the message traffic in coordination
Portion of Total Messages
Portion of Vulnerabilities
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%



Cybersecurity Information Sharing: Analysing an Email Corpus of Coordinated Vulnerability Disclosure

Kiran Sridhar, Allen Householder, Jonathan Spring, Daniel W. Woods

Abstract

1 Introduction

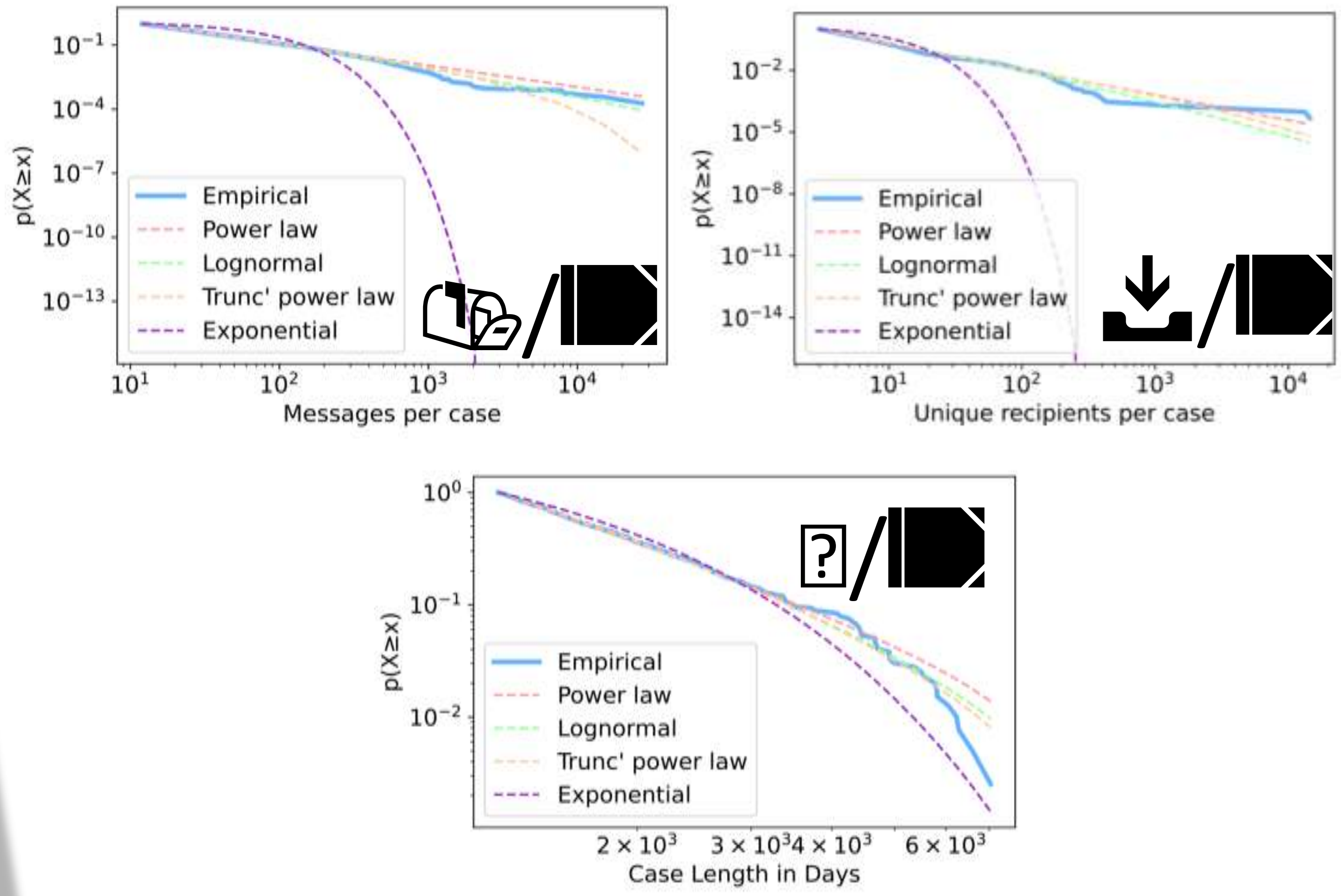
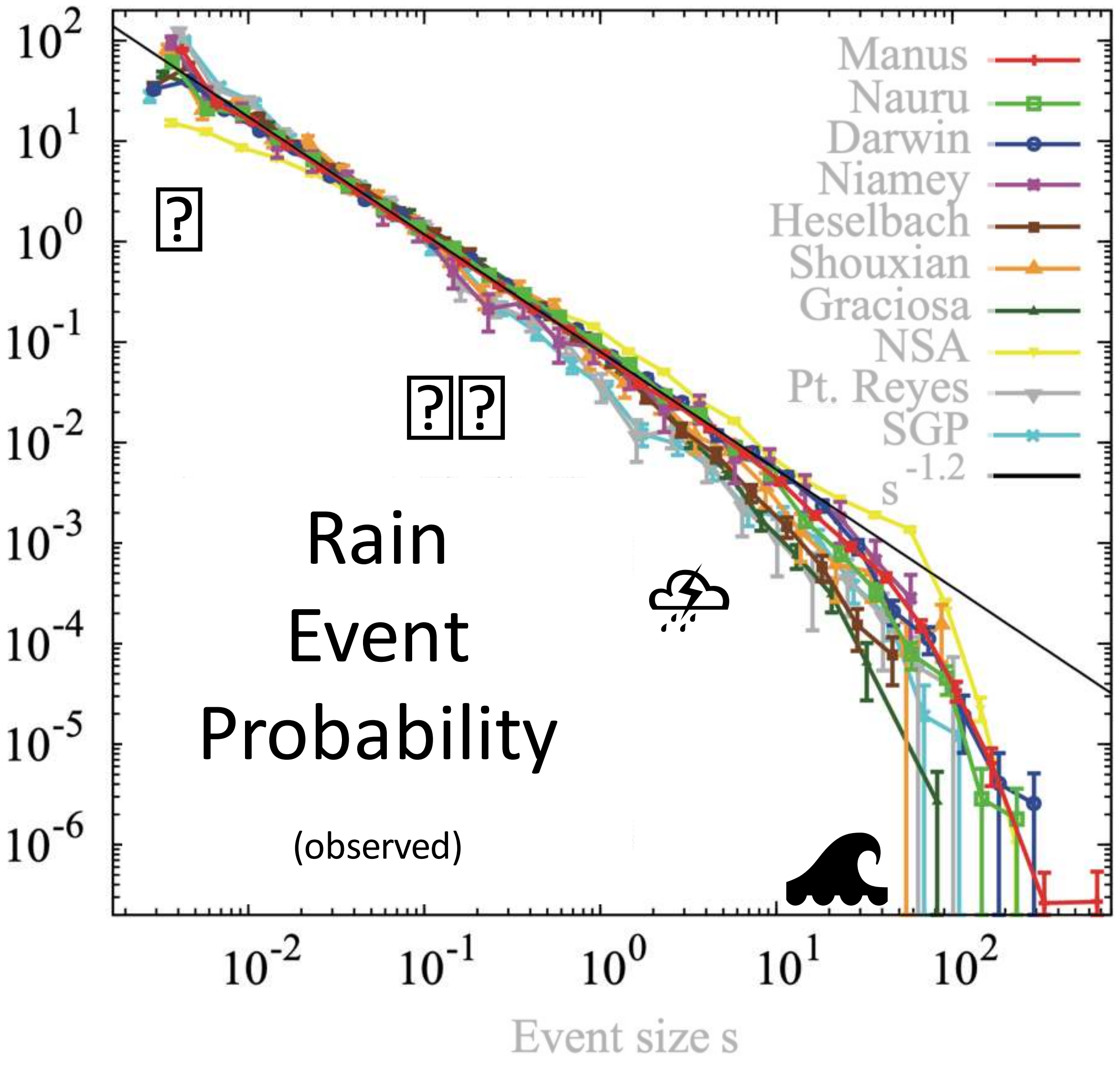


Figure 6: Number of messages and recipients follow a heavy-tailed distribution, whereas the case length in days is much closer to an exponential distribution.

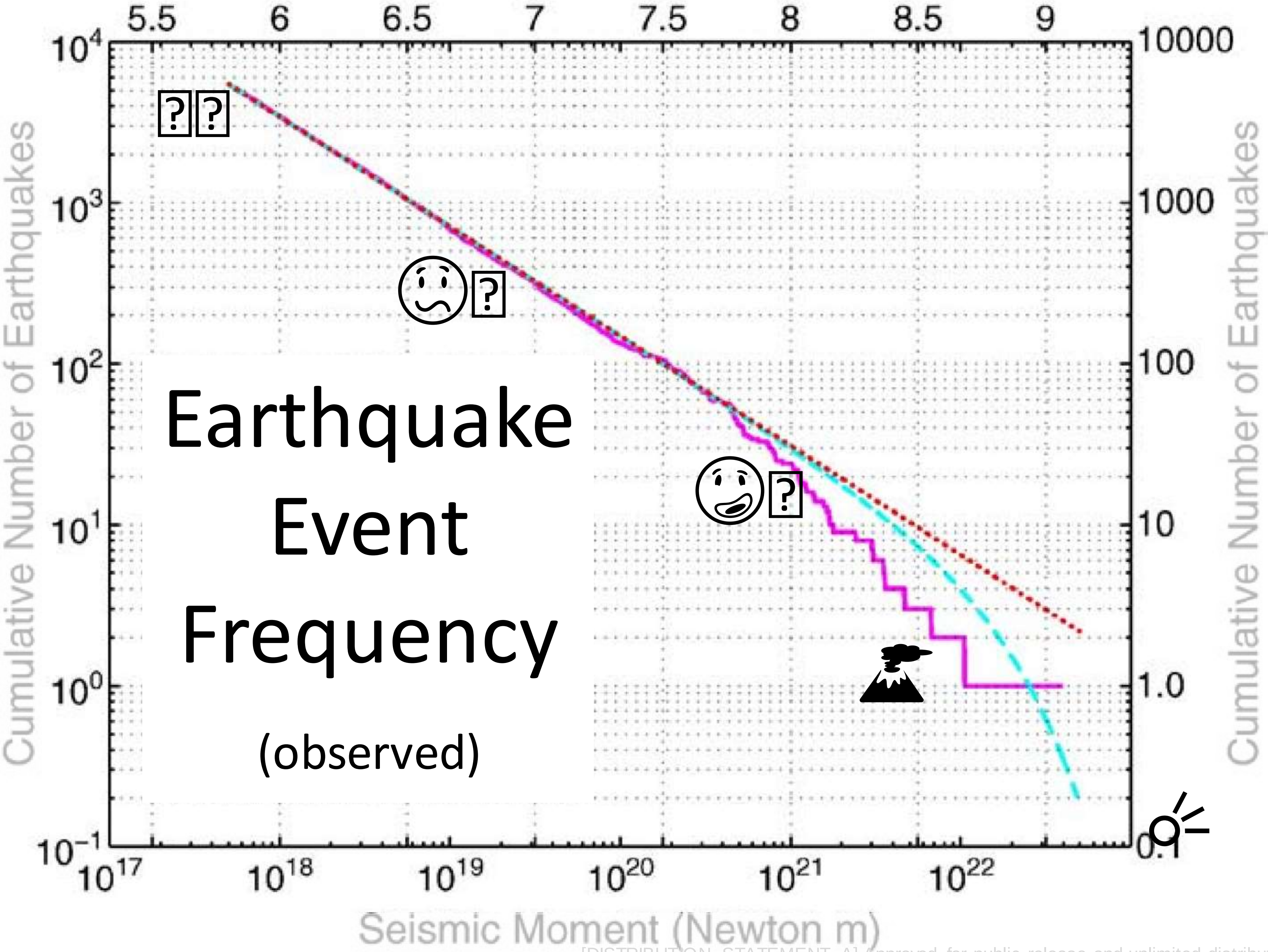
https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-sridhar.pdf



Peters, Ole, et al. "Universality of rain event size distributions." *Journal of Statistical Mechanics: Theory and Experiment* 2010.11 (2010): P11030.
https://arxiv.org/abs/1010.4201

Earthquake Event Frequency

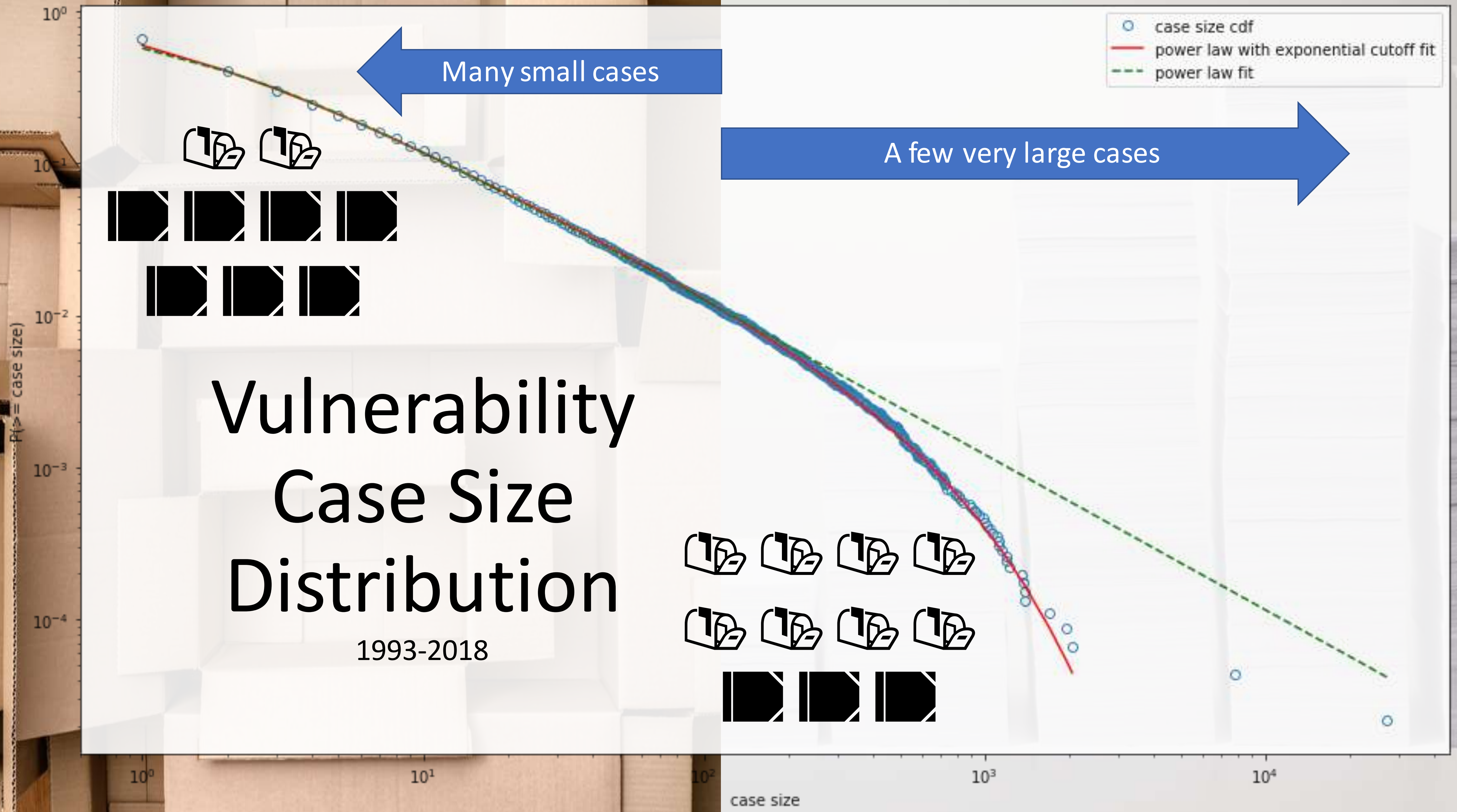
(observed)

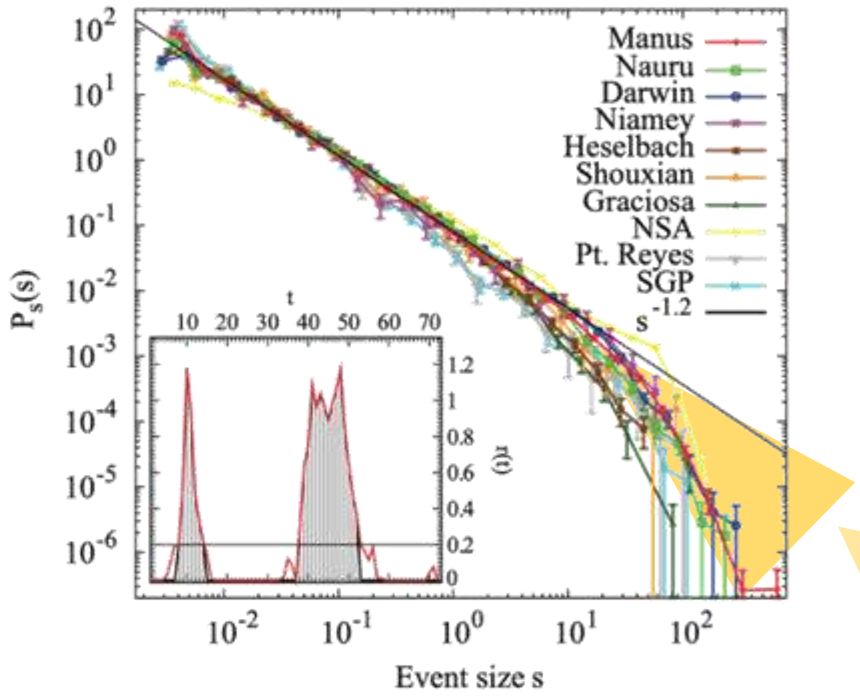


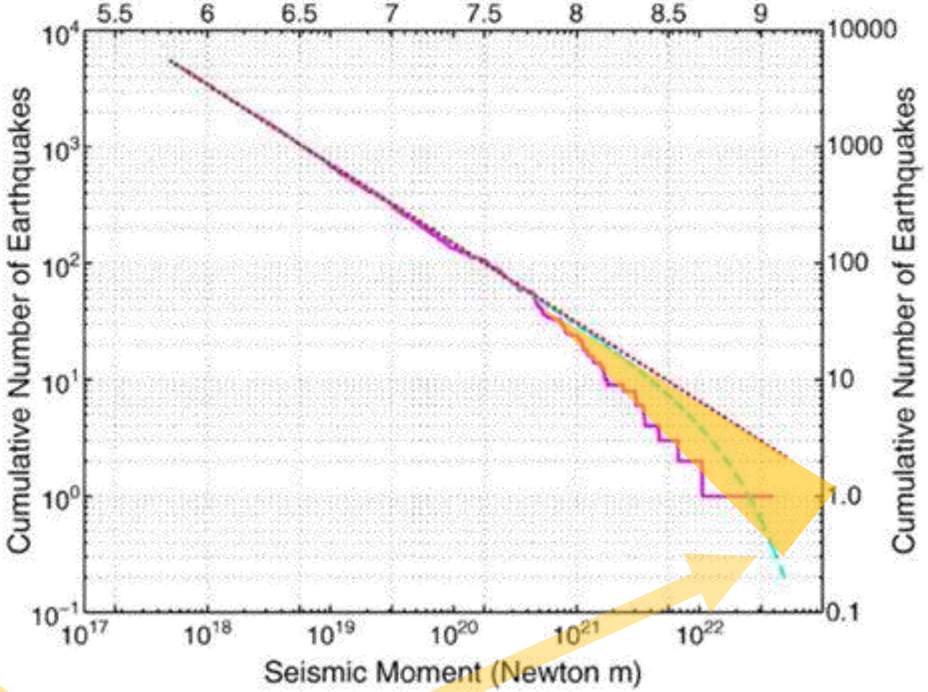
Kagan, Yan Y. "Earthquake size distribution: Power-law with exponent β≡ 12?." *Tectonophysics* 490.1-2 (2010): 103-114. https://doi.org/10.1016/j.tecto.2010.04.034

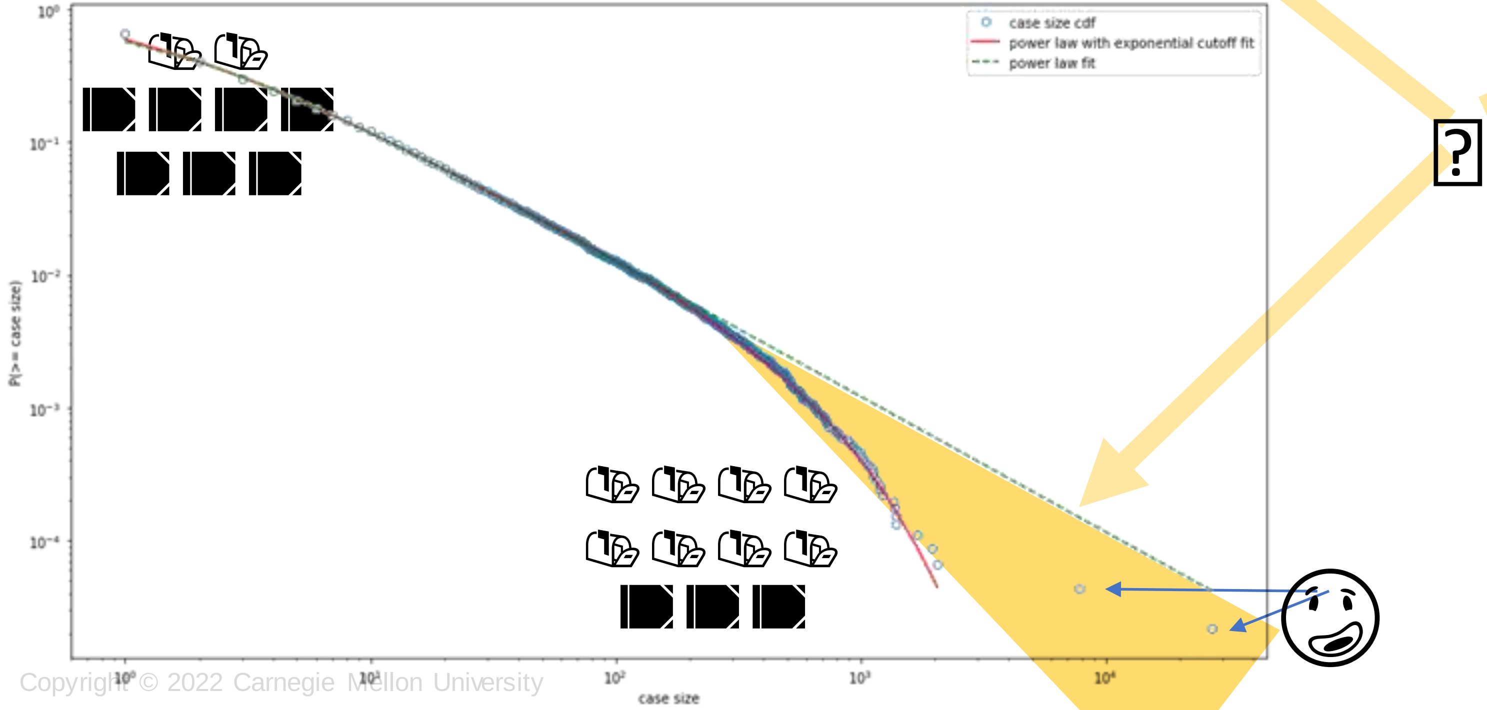
Vulnerability Case Size Distribution

1993-2018



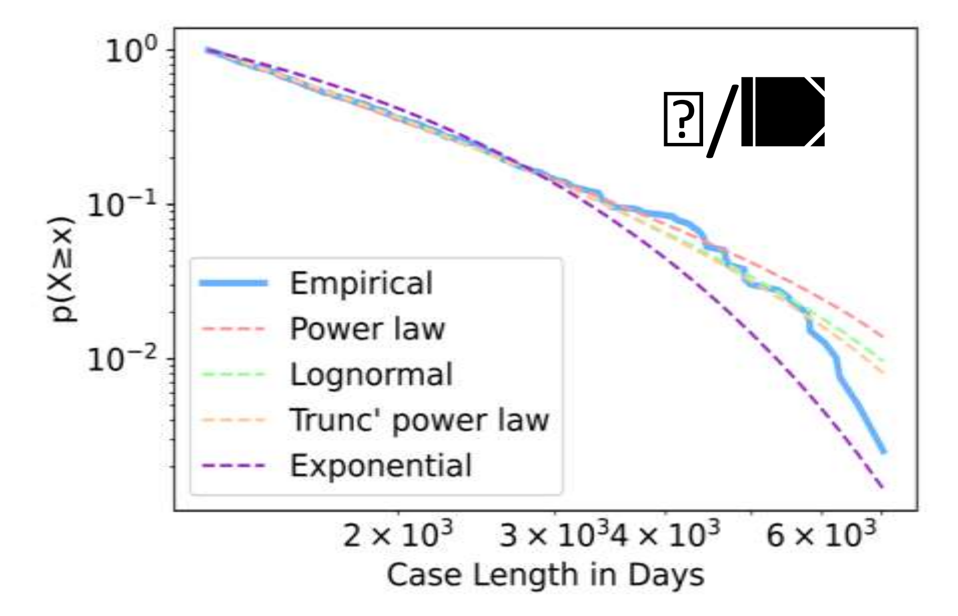




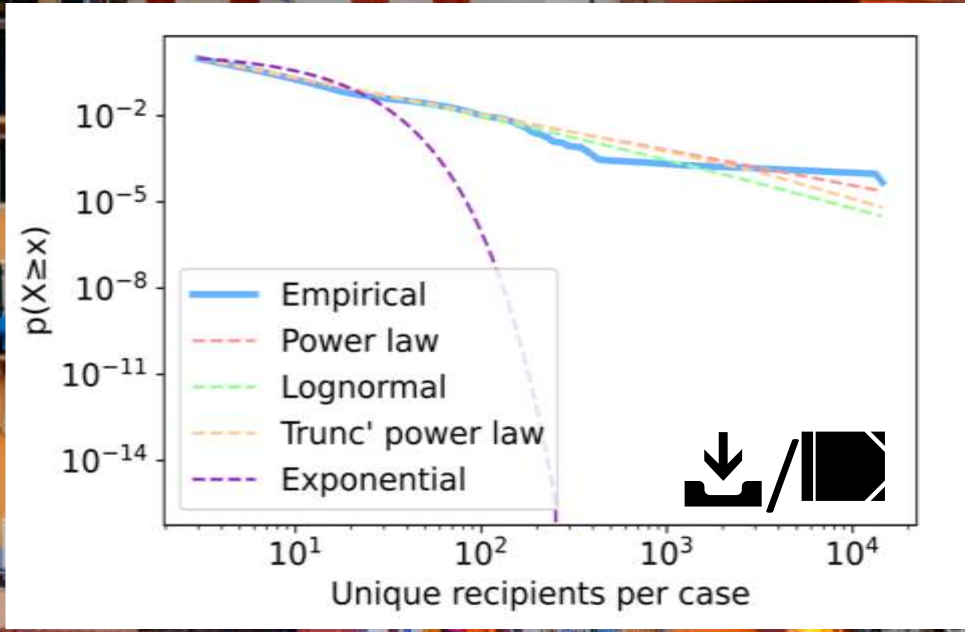


Why is this gap here?

1. Structural Limits
2. Limited Observations

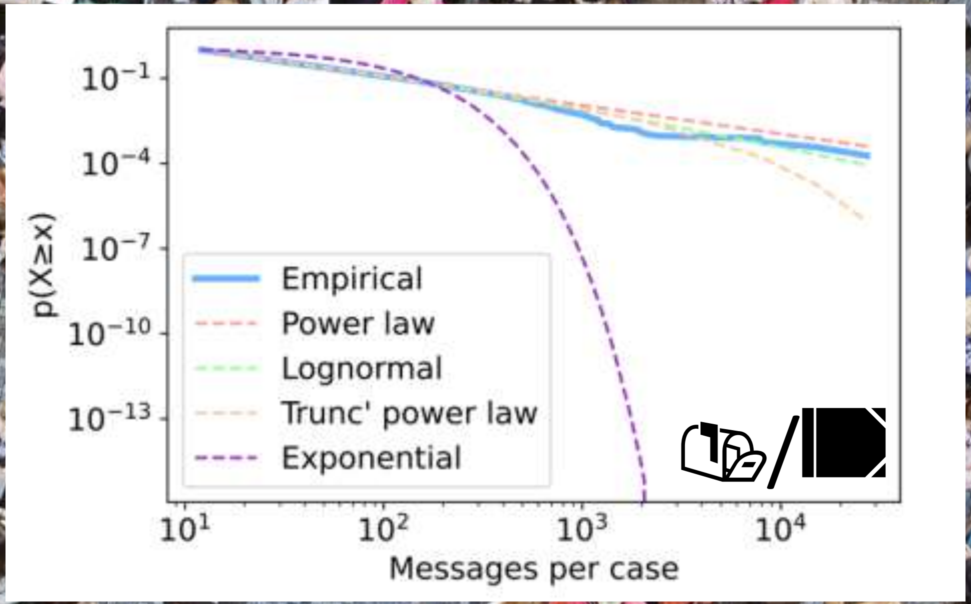


Structural Limit #1
Case Timespan

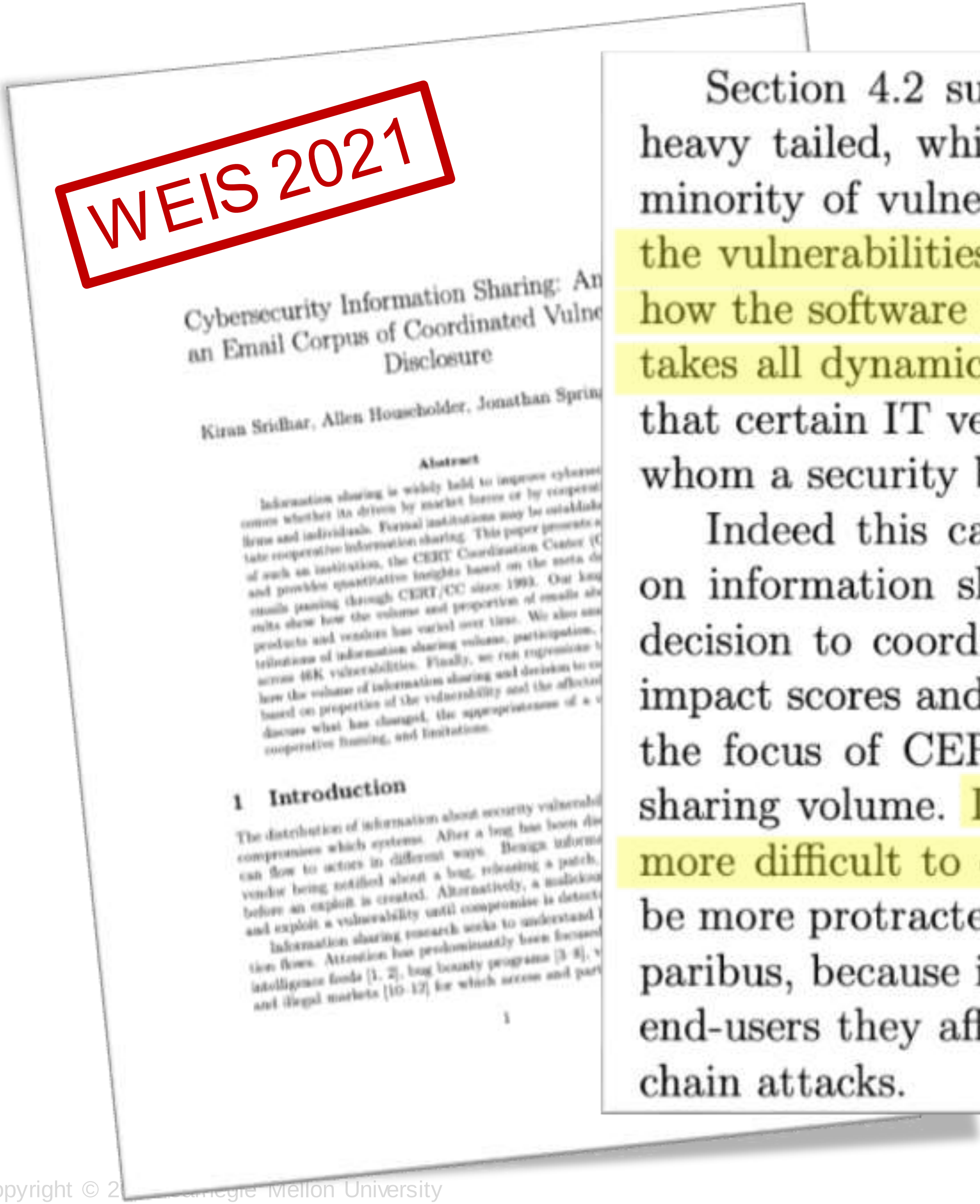


Structural Limit #2

Identifying Affected Vendors



Structural Limit #3
Coordination



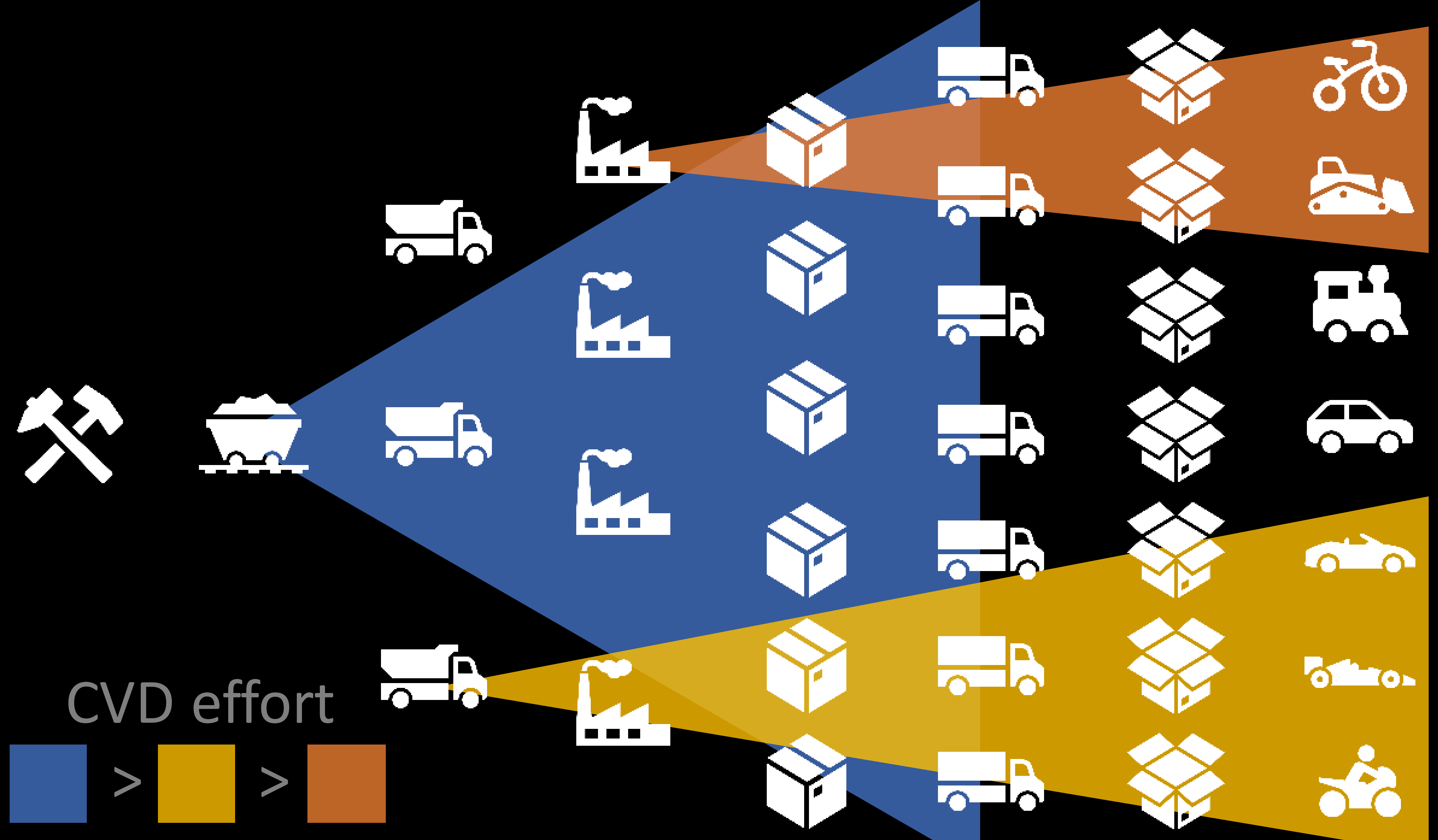
Section 4.2 suggests information sharing volume and participation are heavy tailed, which means the majority of information is shared about a minority of vulnerabilities. This is unlikely down to intrinsic properties of the vulnerabilities, such as those captured by CVSS, but rather because of how the software products are deployed in the world, specifically the winner takes all dynamics of software markets [67]. Tuverson and Ruffle [68] note that certain IT vendors are "systemically important technology entities" for whom a security bug could impact thousands of businesses.

Indeed this can be seen in comparing the effect of proxies for severity on information sharing volume (Table 3) with the effect on CERT/CC's decision to coordinate (Table 4). While vulnerabilities with higher CVSS impact scores and publicly available exploit codes are more likely to become the focus of CERT/CC attention, they do not lead to more information sharing volume. In contrast, upstream supply chain vulnerabilities do seem more difficult to coordinate. Communications about these bugs appear to be more protracted than communications about other vulnerabilities, ceteris paribus, because it takes longer to understand their full scope and all of the end-users they afflict. Indeed, this is consistent with multiple noted supply chain attacks.

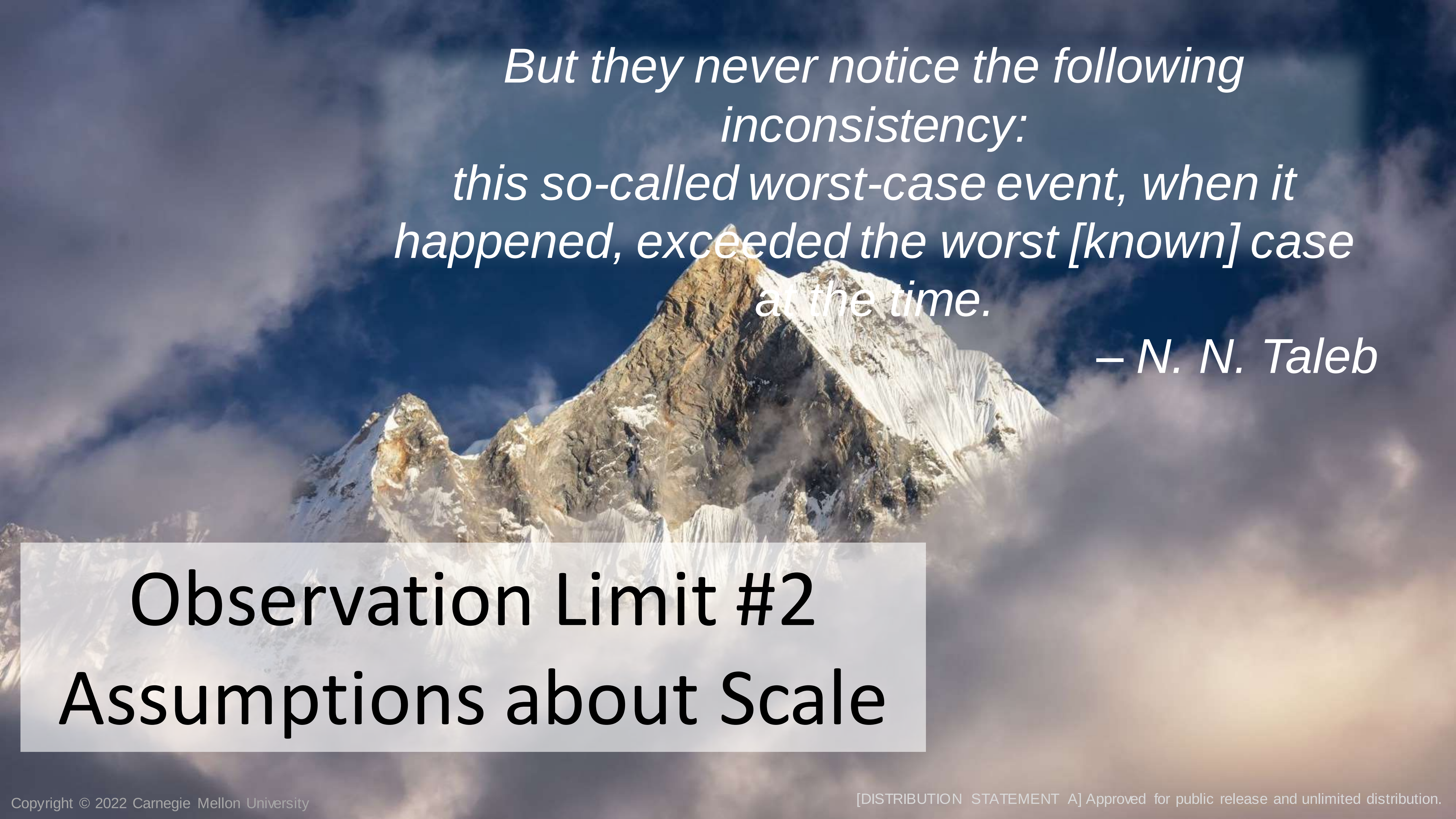
https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-sridhar.pdf


More comms, longer cases


More comms, longer cases


CVD effort
>
>

Observation Limit #1
Limited Data


But they never notice the following inconsistency:
this so-called worst-case event, when it happened, exceeded the worst [known] case at the time.
– N. N. Taleb
Observation Limit #2
Assumptions about Scale

Understand the limits of your observations *and* what they imply for predictions based on them

CVD capacity

Don't build ~~stormwater mitigation~~ based on average ~~rainfall~~

^ case workloads

Build for worse than you've seen.

Accept that sometimes you might still be wrong.

Allen Householder

adh@cert.org

@__adh__

For more:

CERT Guide to CVD

Ubiquity
Mark Buchanan

Antifragile
Nassim Nicholas Taleb