

Allen
Householder
CERT/CC
@__adh__

Like vuls in rain

Copyright 2022 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM22-0078



Coordinated Vulnerability Disclosure (CVD) at CERT/CC

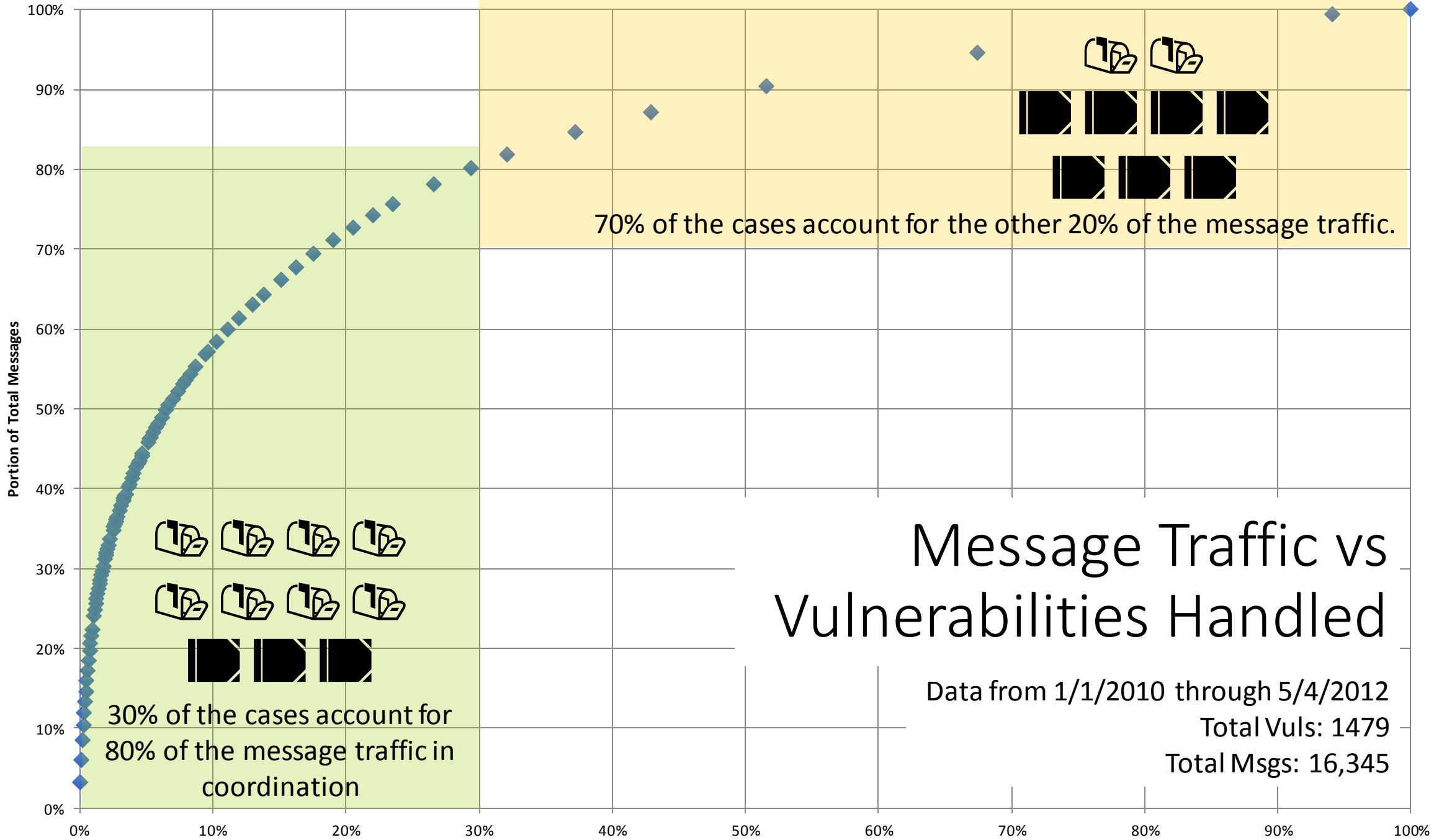
Email data set spans 1993-2020

 434k messages

 46k vulnerability cases

 250 vendors

  ( + ) /  ?



WEIS 2021

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

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

Abstract

Information sharing is widely held to improve cybersecurity outcomes whether its driven by market forces or by cooperation among firms and individuals. Formal institutions may be established to facilitate cooperative information sharing. This paper presents a case-study of such an institution, the CERT Coordination Center (CERT/CC), and provides quantitative insights based on the meta data of 434K emails passing through CERT/CC since 1993. Our longitudinal results show how the volume and proportion of emails about different products and vendors has varied over time. We also analyse the distribution of information sharing volume, participation, and duration across 66K vulnerabilities. Finally, we run regressions to understand how the volume of information sharing and duration is correlated with based on properties of the vulnerability and the affected vendor. We discuss what has changed, the appropriateness of a competitive or cooperative framing, and limitations.

1 Introduction

The distribution of information about security vulnerabilities determines who compromises which systems. After a bug has been discovered, information can flow to actors in different ways. Benign information flows include a vendor being notified about a bug, releasing a patch, and it being applied before an exploit is created. Alternatively, a malicious actor could discover and exploit a vulnerability until compromise is detected. Information sharing research seeks to understand how and why information flows. Attention has predominantly been focused on proprietary threat intelligence feeds [1, 2], bug bounty programs [3–5], vulnerability credits [6], and illegal markets [10–12] for which access and participation are driven by

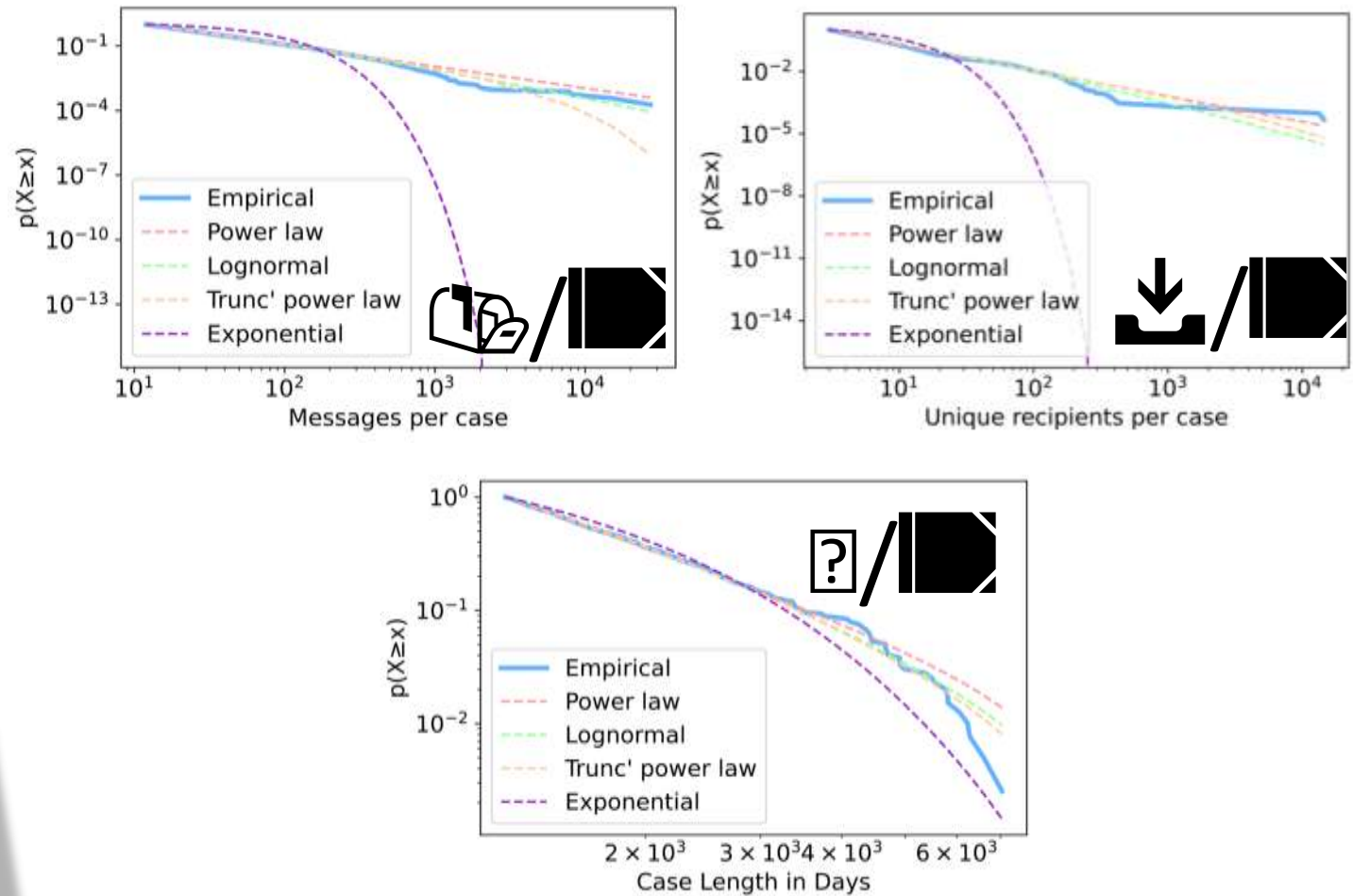
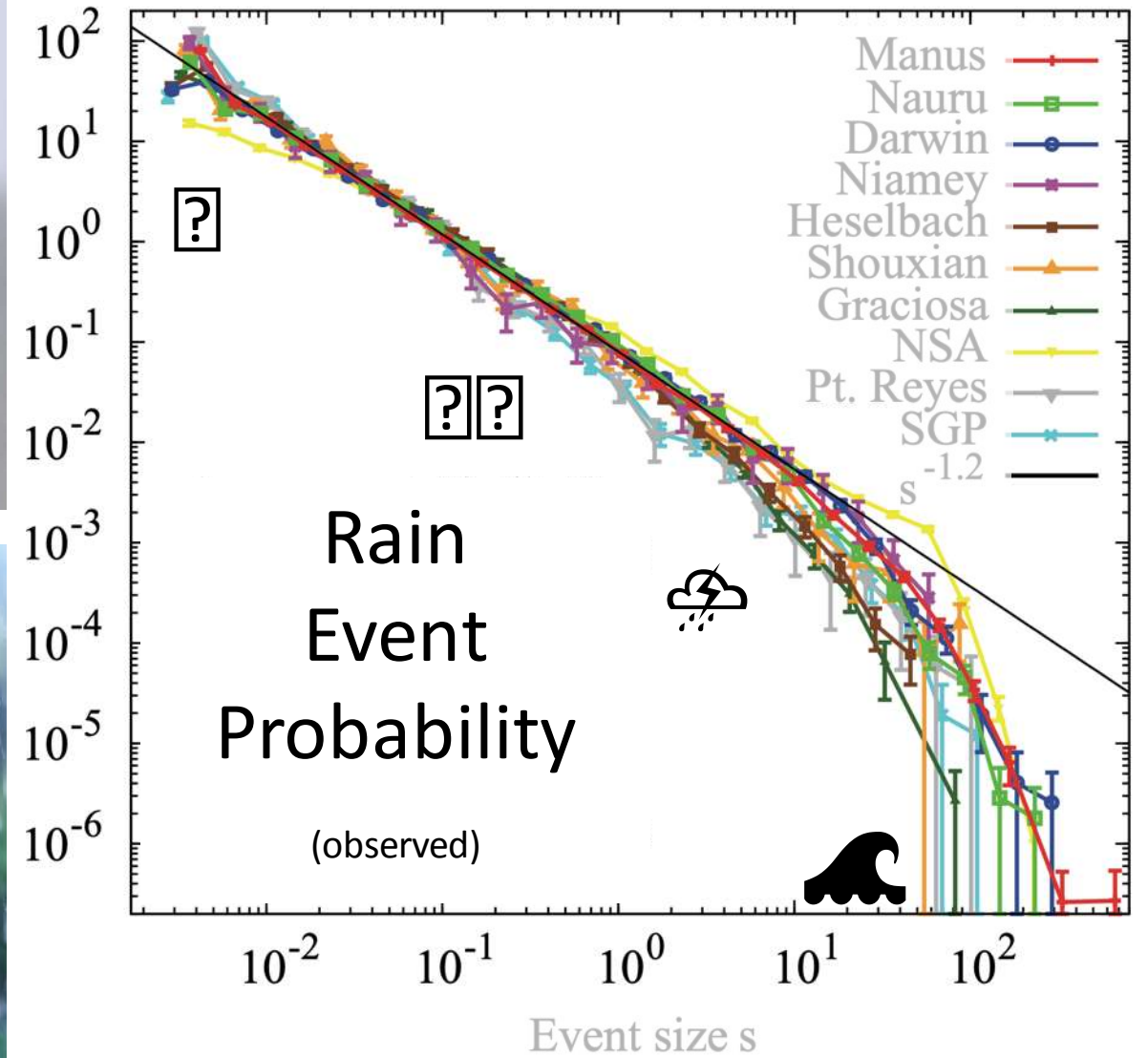


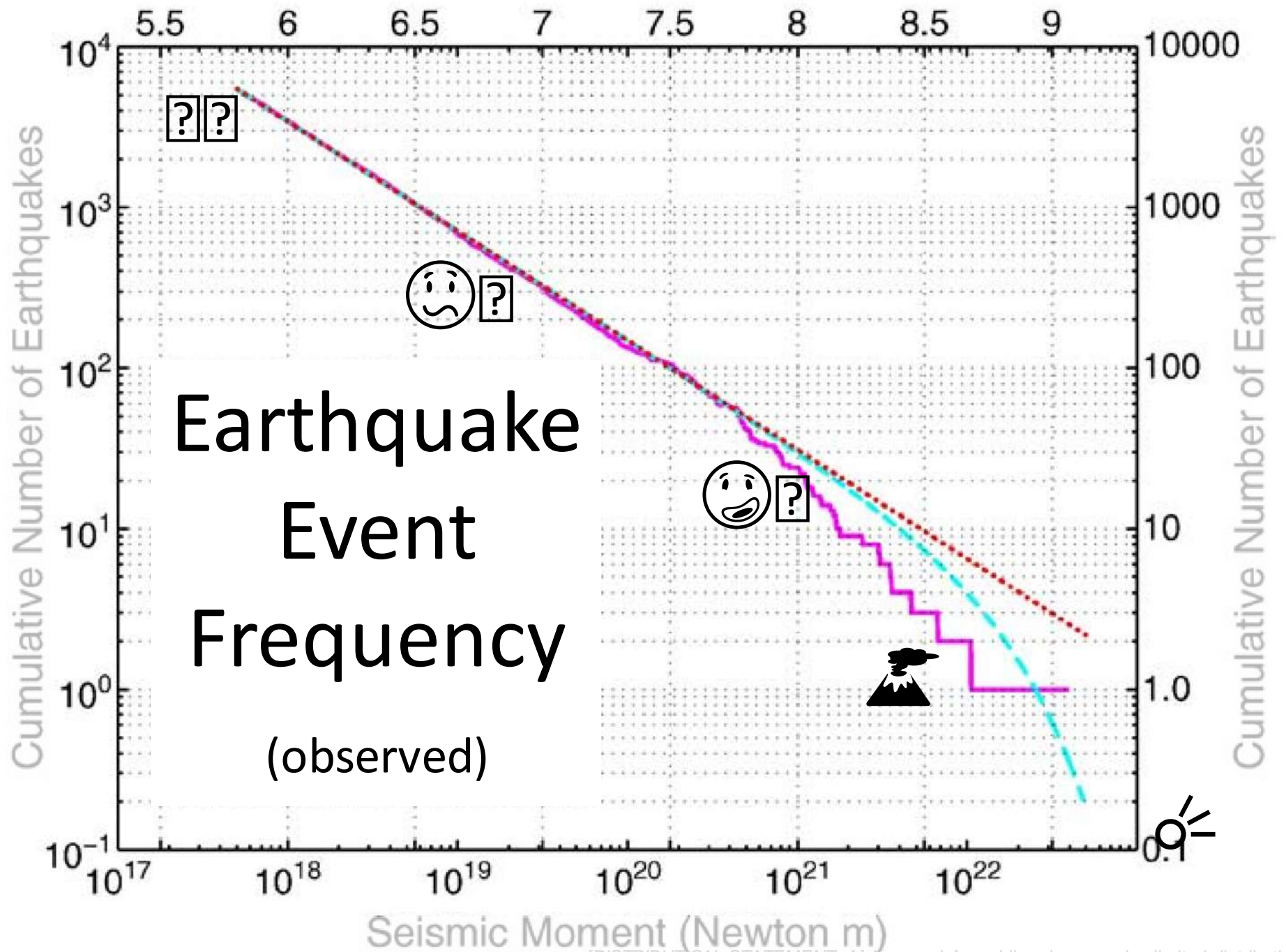
Figure 6: Number of messages and recipients follow a heavy-tailed distribution, whereas the case length in days is much closer to an exponential distribution.

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

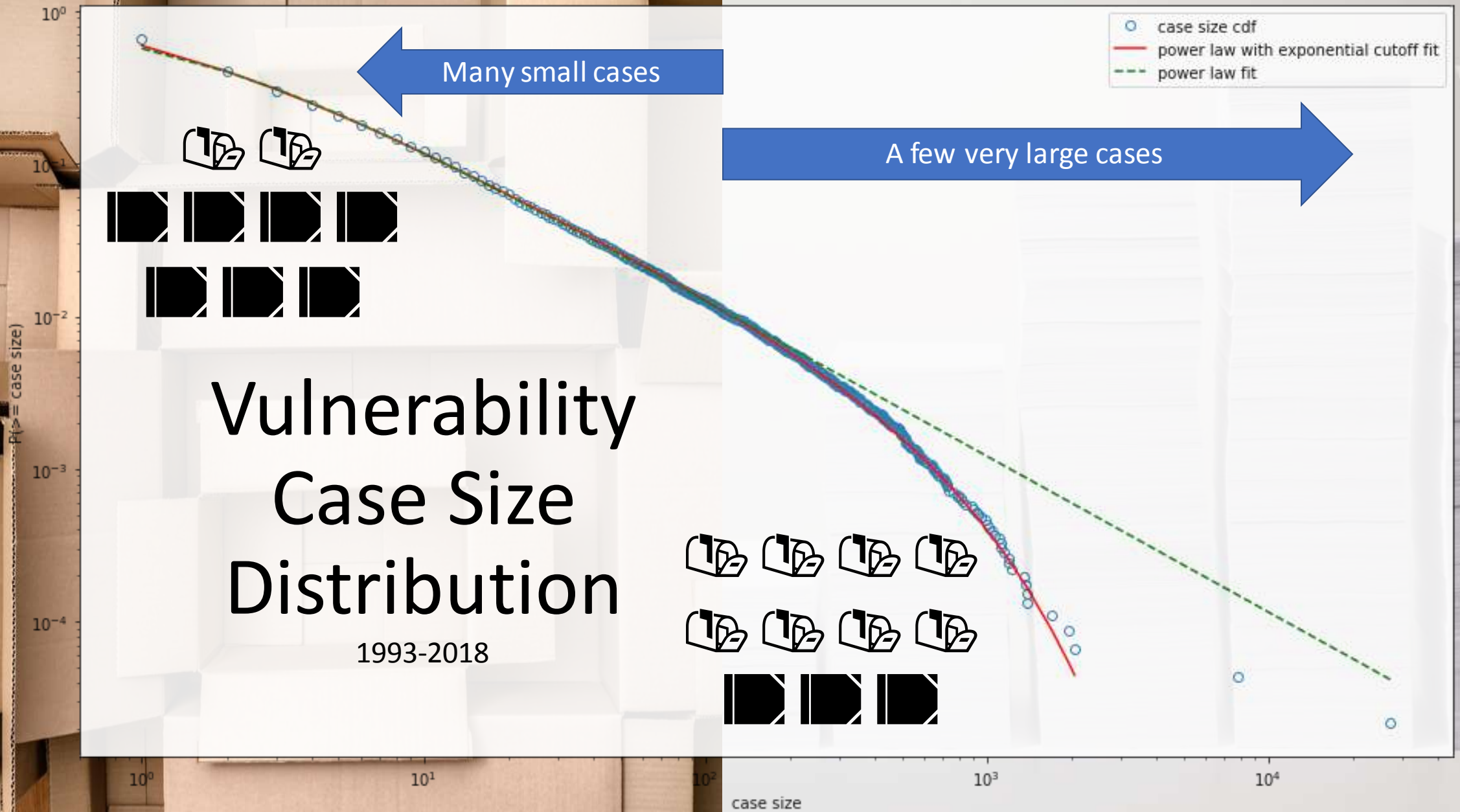


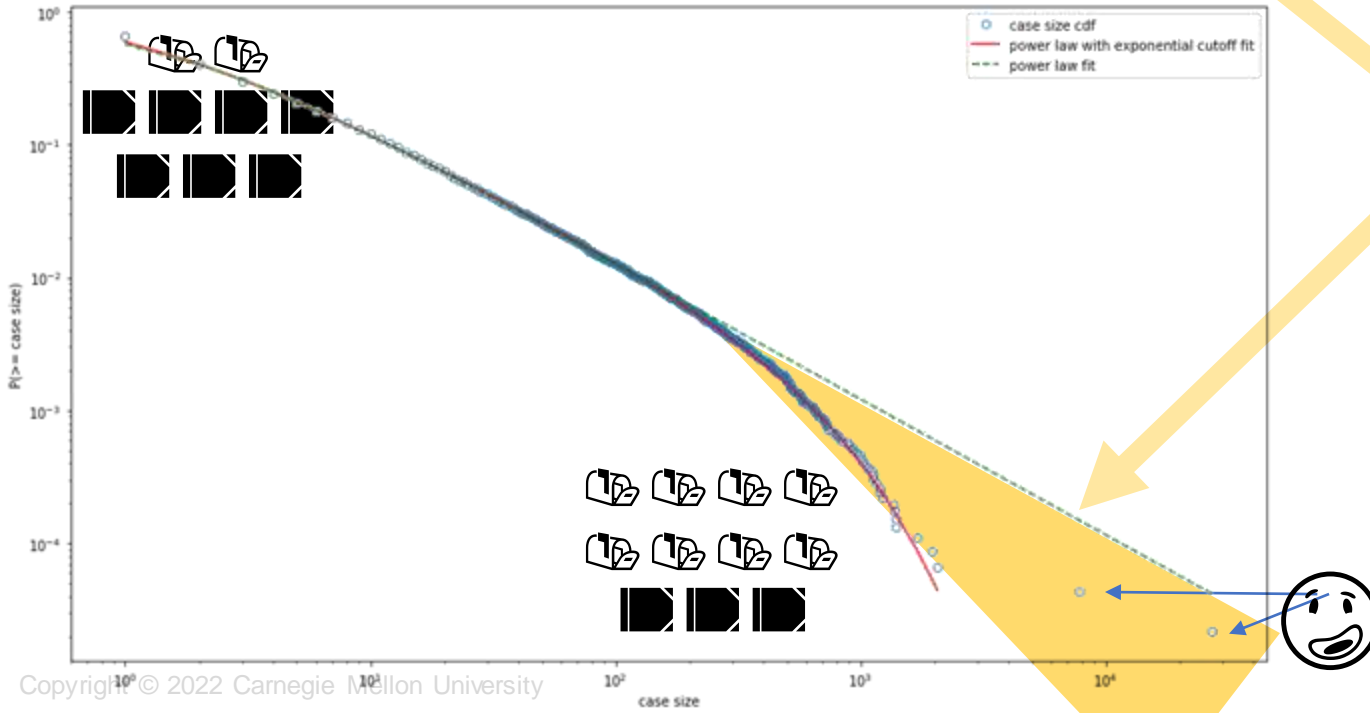
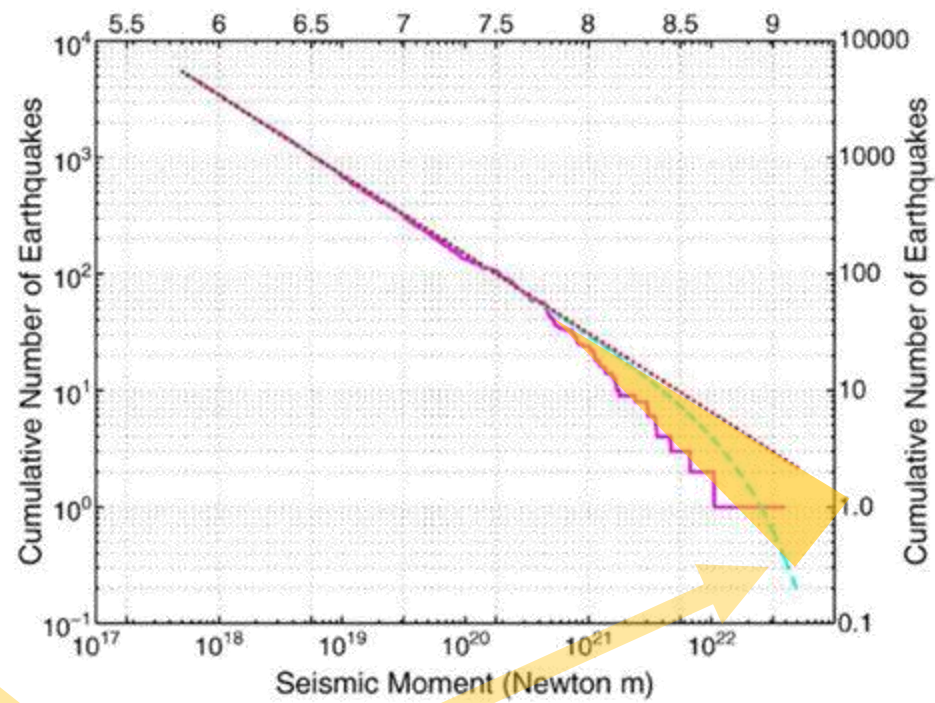
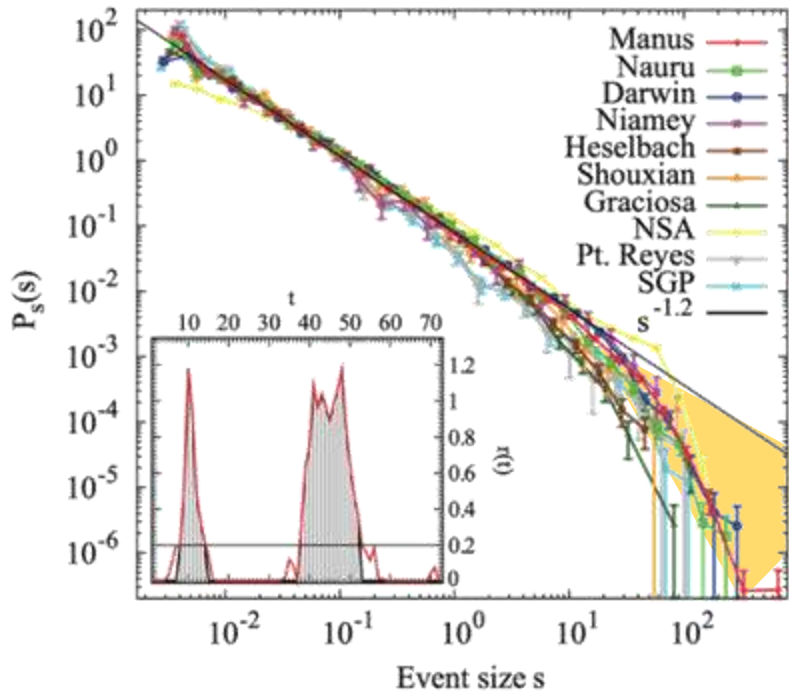
Peters, Ole, et al. "Universality of rain event size distributions." *Journal of Statistical Mechanics: Theory and Experiment* 2010.11 (2010): P11030.

<https://arxiv.org/abs/1010.4201>



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



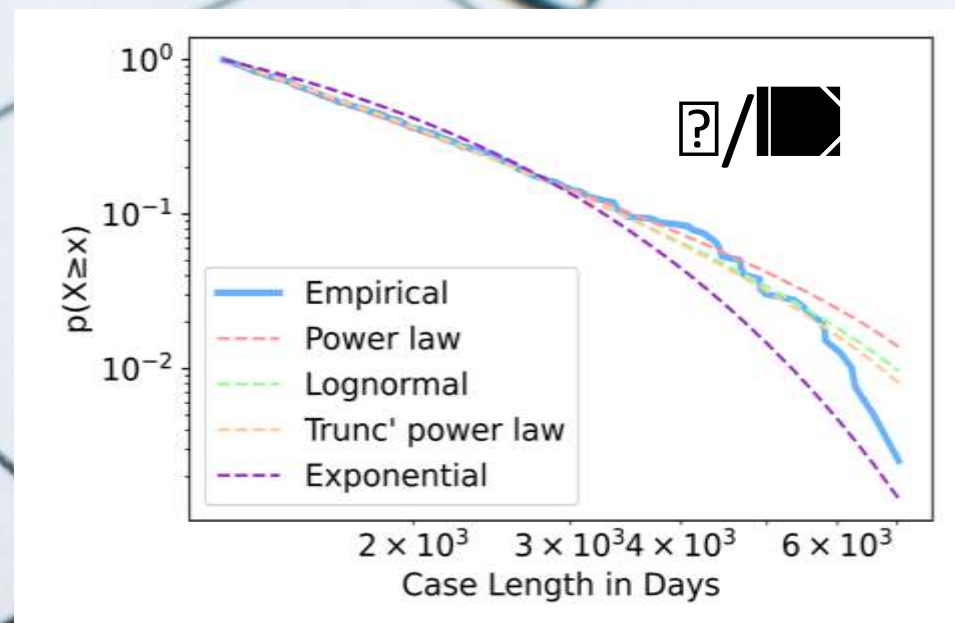


? Why is this gap here?

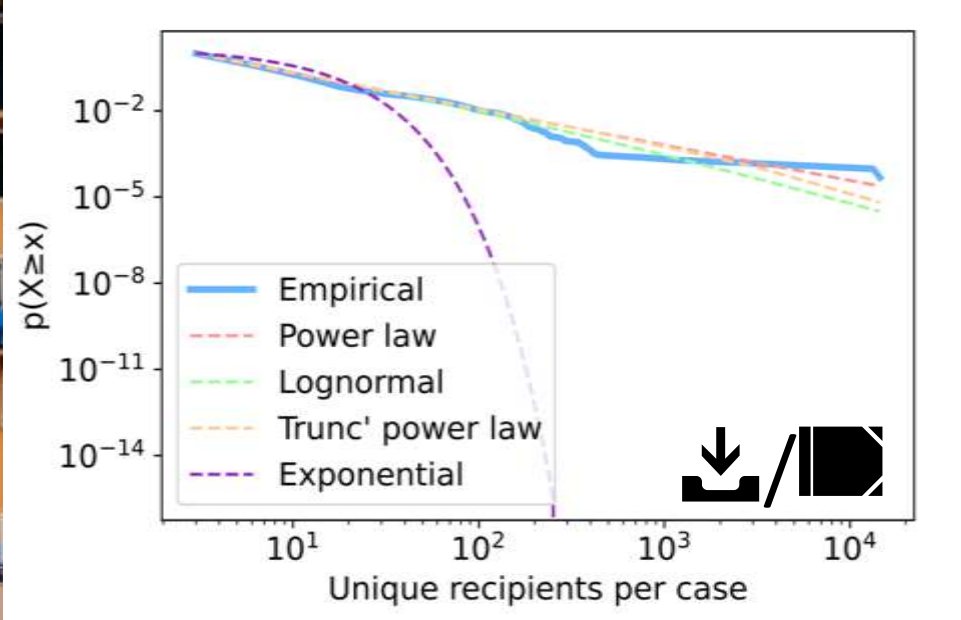
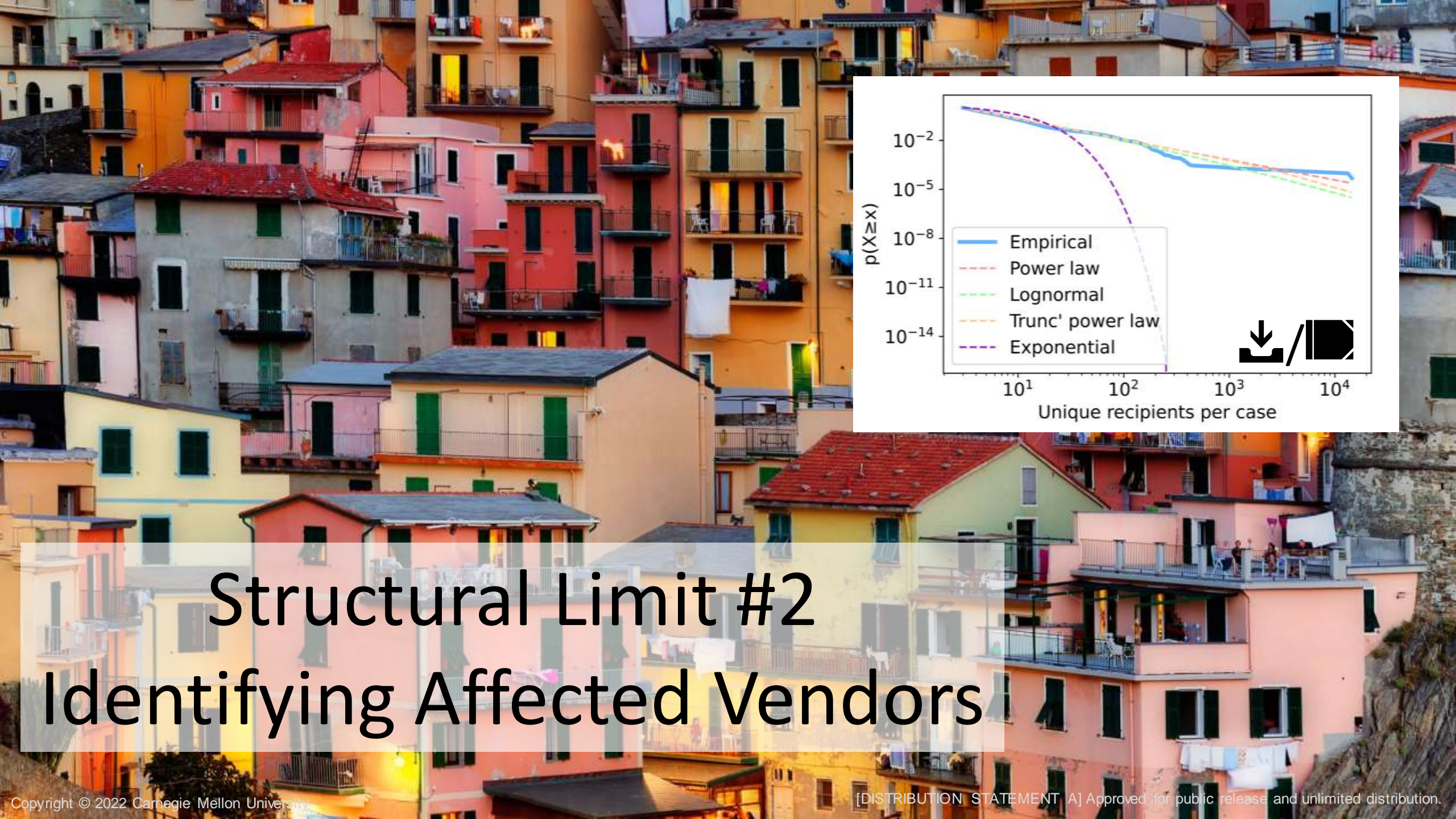
1. Structural Limits

2. Limited Observations

MONDAY

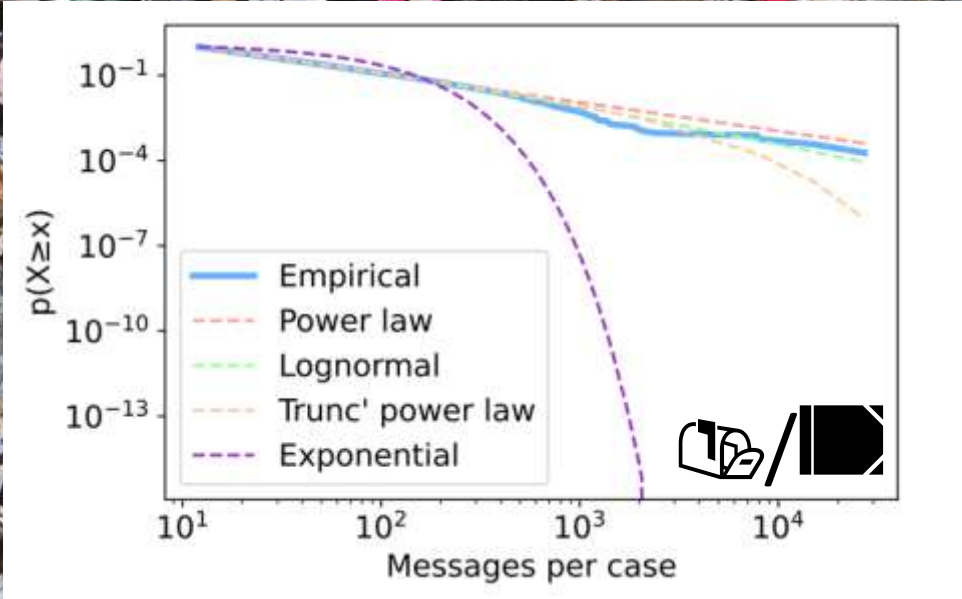
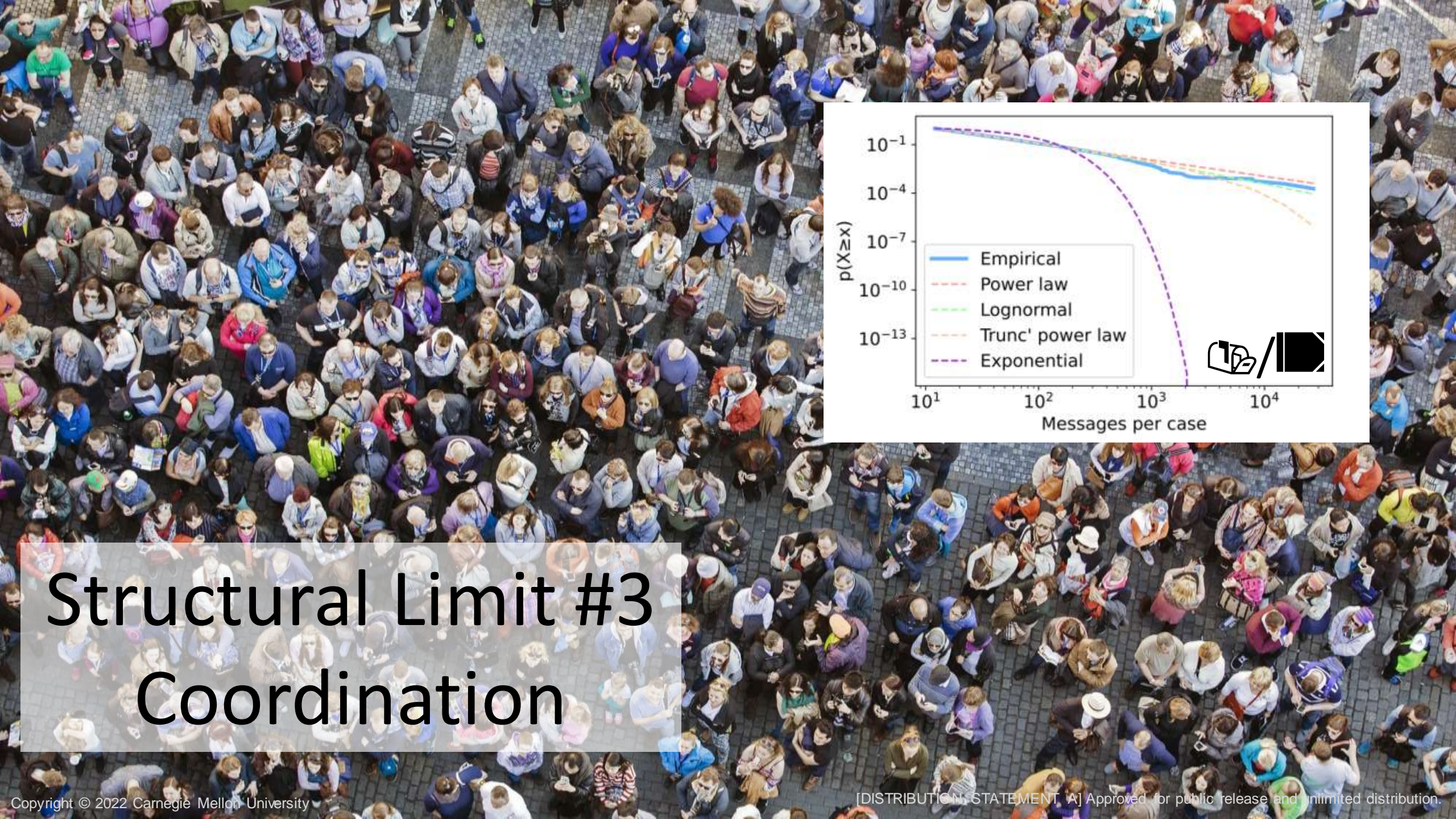


Structural Limit #1 Case Timespan



Structural Limit #2

Identifying Affected Vendors



Structural Limit #3 Coordination

WEIS 2021

Cybersecurity Information Sharing: An Email Corpus of Coordinated Vulnerability Disclosure

Kiran Sridhar, Allen Householder, Jonathan Spring

Abstract

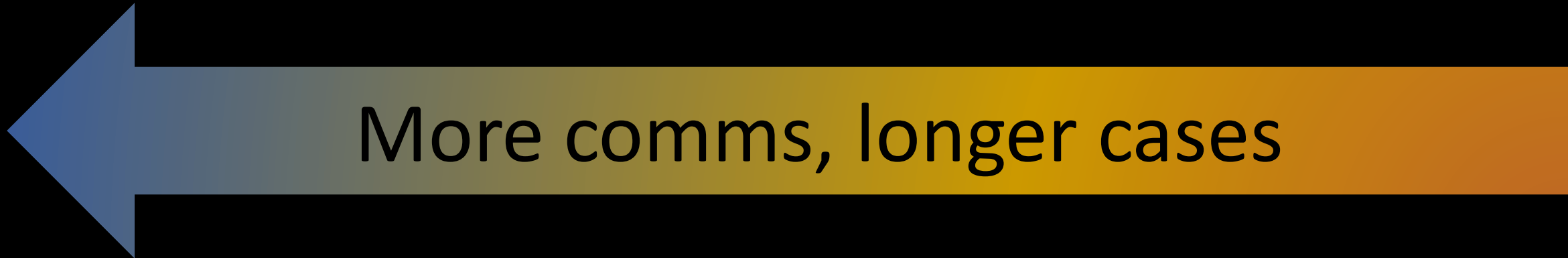
Information sharing is widely held to improve cybersecurity across whether its driven by market forces or by corporate firms and individuals. Formal institutions may be outtake take cooperative information sharing. This paper presents a study of such an institution, the CERT Coordination Center (CERT/CC) and provides quantitative insights based on the meta data of emails passing through CERT/CC since 1993. Our key results show how the volume and proportion of emails about products and vendors has varied over time. We also see variations of information sharing volume, participation, across 66K vulnerabilities. Finally, we run regressions to show the volume of information sharing and decision to disclose based on properties of the vulnerability and the affected discuss what has changed, the appropriateness of a cooperative framing, and limitations.

1 Introduction

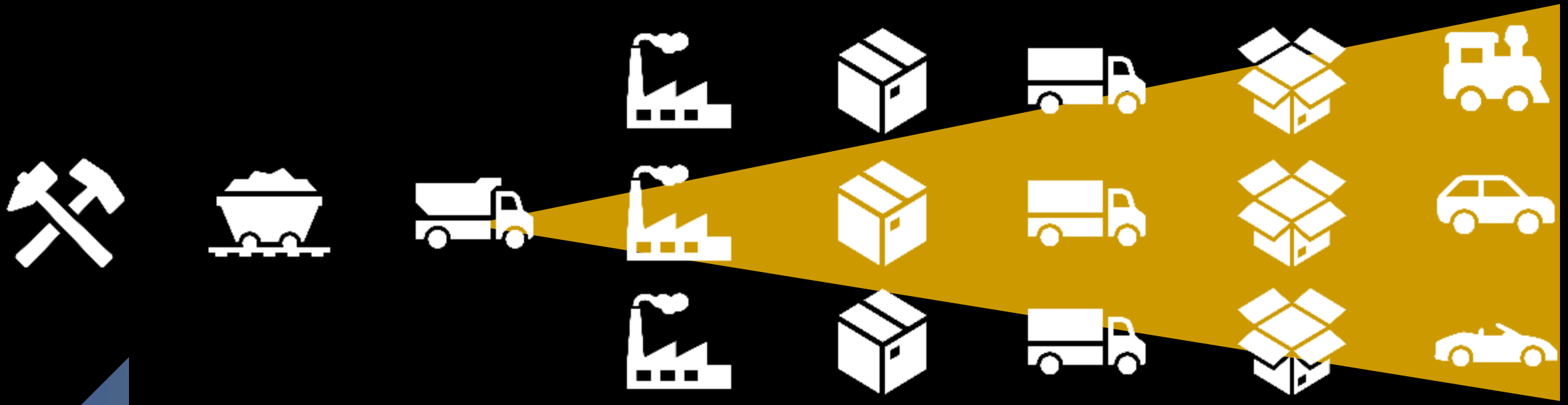
The distribution of information about security vulnerabilities and compromises which systems. After a bug has been discovered, information can flow to actors in different ways. benign informants, vendor being notified about a bug, releasing a patch, before an exploit is created. Alternatively, a malicious actor may detect and exploit a vulnerability until compromise is detected. Information sharing research seeks to understand information flows. Attention has predominantly been focused on intelligence feeds [1, 2], bug bounty programs [3–6], and illegal markets [10–12] for which access and part

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.



More comms, longer cases



More comms, longer cases



CVD effort



>



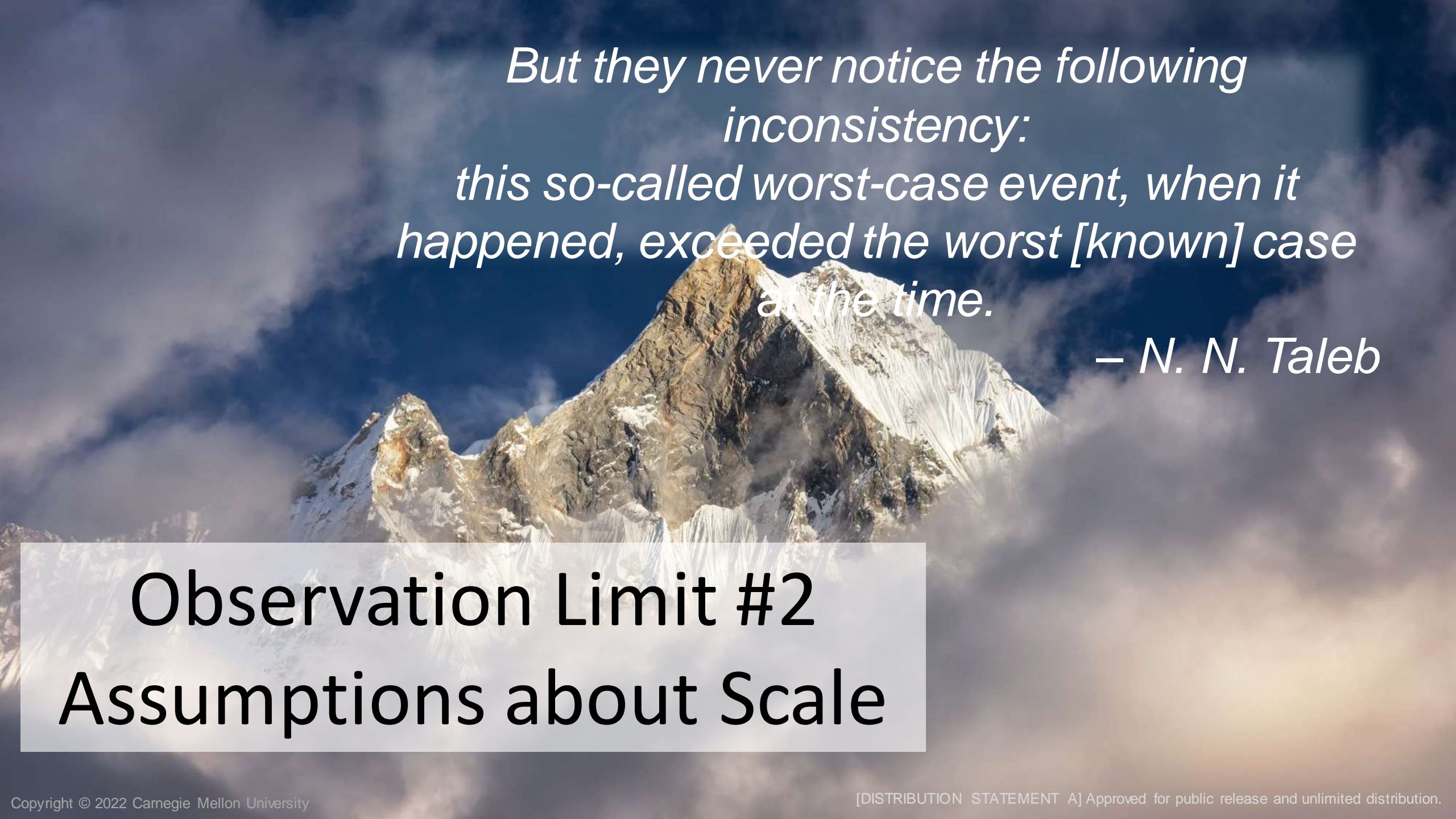
>



A close-up photograph of a person with long brown hair looking through black binoculars. The person is wearing a blue and white striped shirt. The background is a bright, sunny outdoor setting with a clear blue sky and a blurred horizon line. The binoculars are held up to the person's eyes, and the lenses are prominent in the foreground.

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

Don't build ~~stormwater mitigation~~ based on average rainfall
^{CVD capacity}
^{^ 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