The Risk of a Cyber Disaster:

Estimating the Exceedance Probability Function of a Global Computer Virus

CYBER2021: Manuscript # 80049

Vaughn H. Standley
National Defense University
Fort Lesley J. McNair
Washington D.C. 20319 USA
email: vaughn.standley@nnsa.doe.gov

Roxanne B. Everetts
National Defense University
Fort Lesley J. McNair
Washington D.C. 20319 USA
email: roxanne.everetts@ndu.edu

Disclaimer

The opinions, conclusions, and recommendations expressed or implied are the authors' and do not necessarily reflect the views of the Department of Defense or any other organization.

Introduction

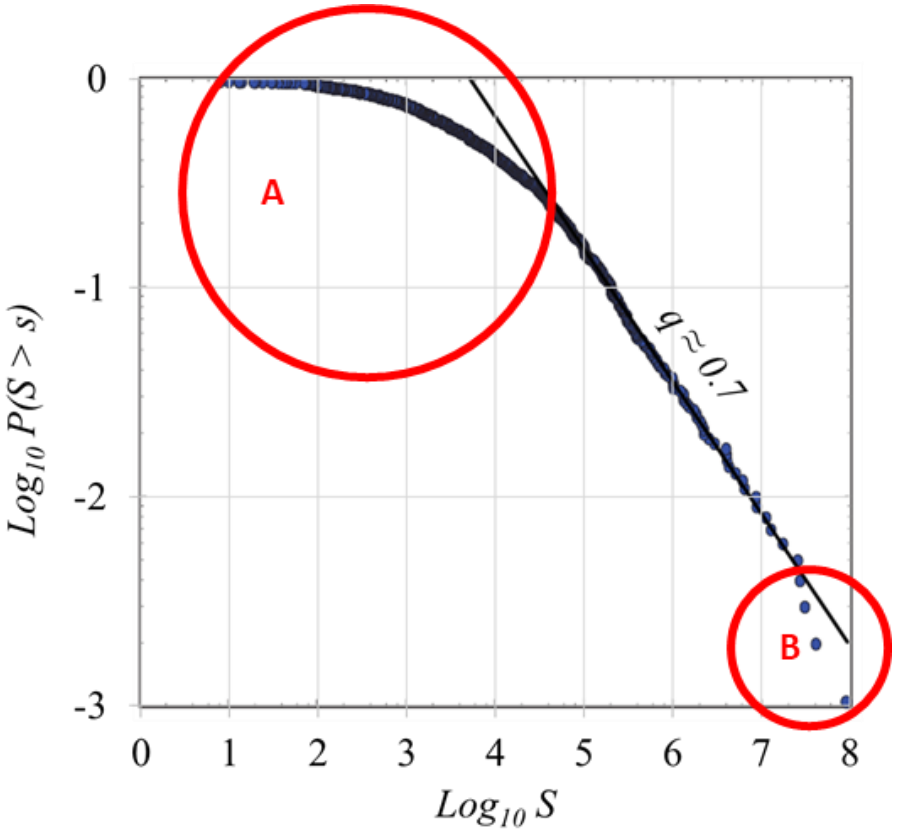
- Risk is the product of probability and severity.
- The Exceedance Probability Function is the mathematical object that associates probability with severity.
- The Power Law is often used erroneously to model exceedance probability.
- Here, an alternative approach is demonstrated using empirical data for interstate war, the coronavirus pandemic, and identity theft. The method relates the frequency distribution of severity S to the product of frequency distributions for vulnerability V, exposure E, and population P. The probability density function for S, from which the exceedance probability function is derived, may then be computed using obtainable distributions for V, E, and P if data for S is not directly available.
- The method is used to estimate the risk of a global cyber disaster.

The Severity S of a Disaster is Described by an Exceedance Probability Function, $P(S>s)$

$$P(S > s) = 1 - P(S \leq s)$$

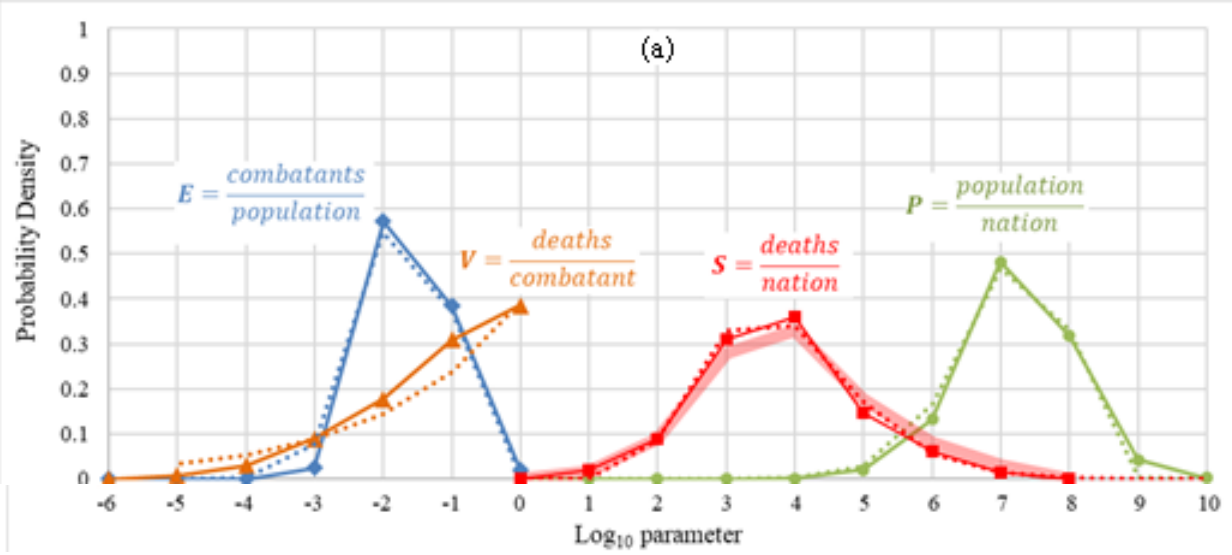
$$= 1 - \int_0^s PDF\ ds$$

- PDF = Probability Density Function
- Power Law, $P(S > s) \approx s^{-q}$, is often misapplied in catastrophe theory:
  - Circles A & B shows large amounts of data is not represented by the law
  - Mathematically divergent when $q<1$



PDFs for Interstate War

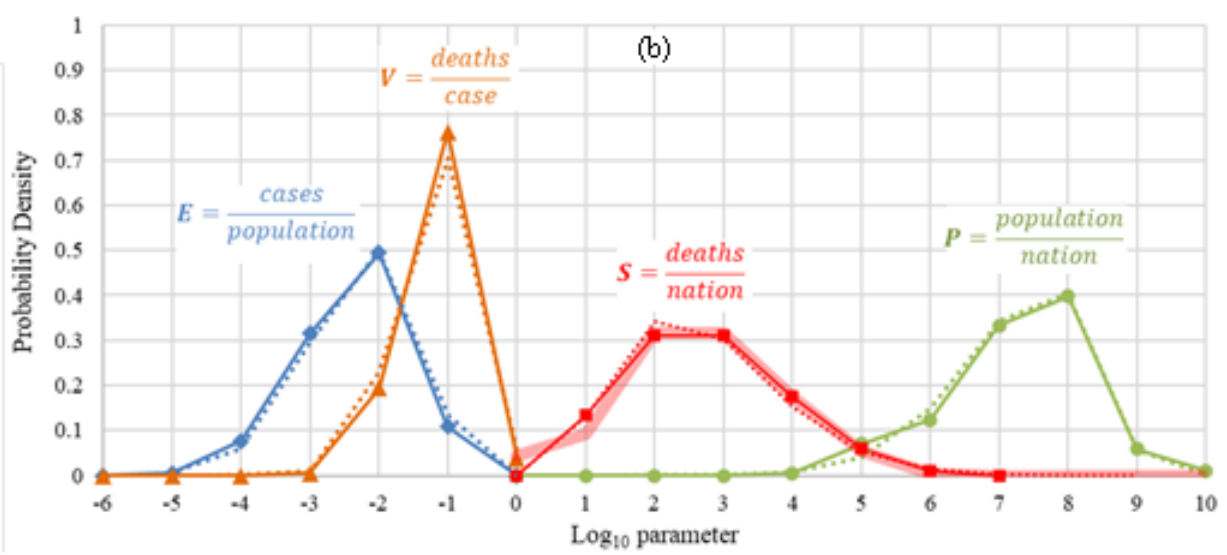
- From Correlates of War (COW) data, the following frequency distributions were determined:
  - Population per state, P
  - Number of combatants per capita, E (i.e., exposure)
  - Deaths per combatant, V *(i.e., vulnerability)*
  - Deaths per nation, S *(i.e., severity)*
- COW data confirms that interstate war severity can be computed using $S=VEP$



PDFs for interstate war. Solid lines with solid markers indicate empirical data, dotted lines with no markers indicate parametric fits to data, and the thick semi-transparent line indicates the curve computed using the relation $S=VEP$.

PDFs for COVID-19

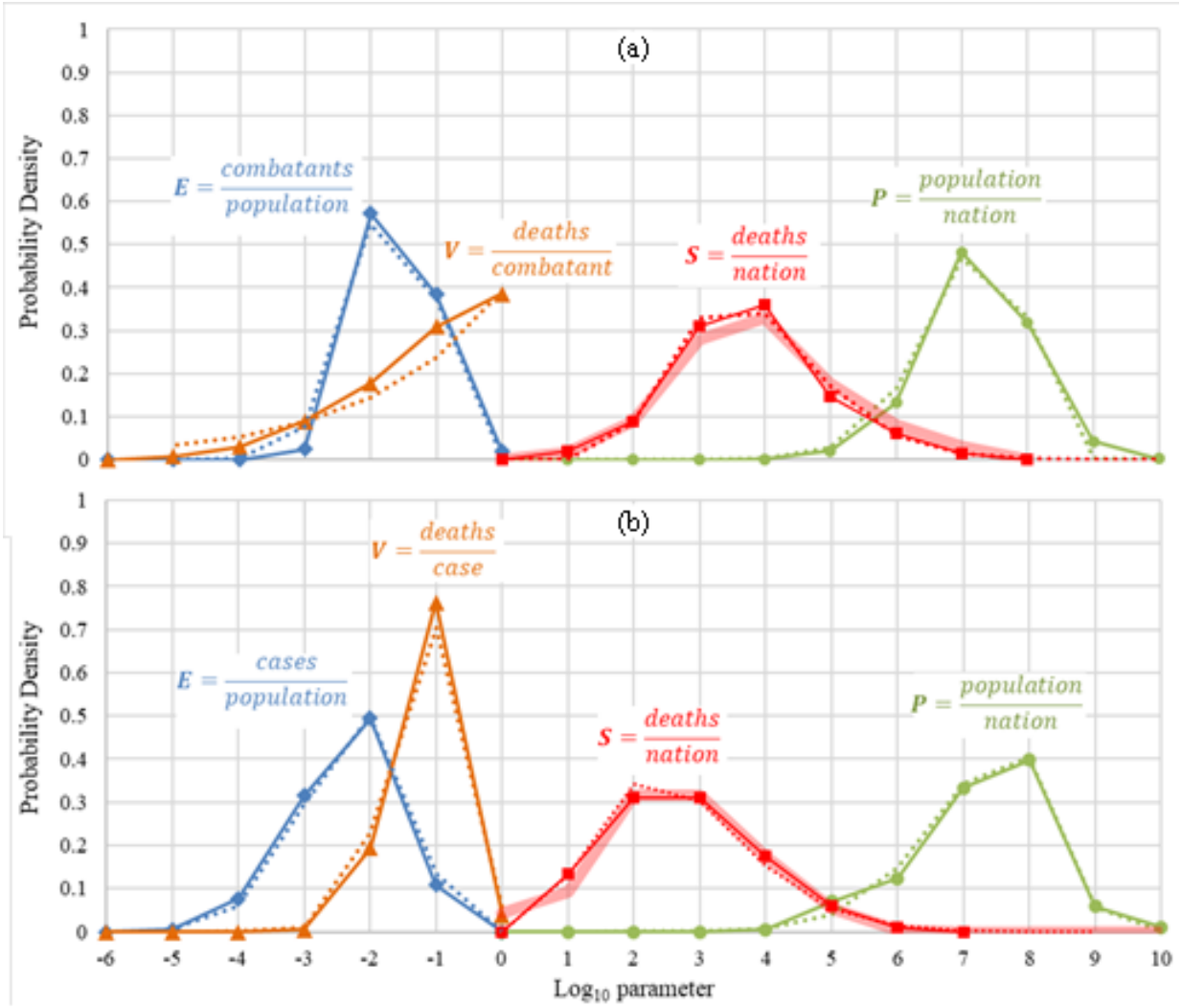
- From Our World in Data (OWID) COVID-19 pandemic data, the following frequency distributions were determined:
  - Population per state, P
  - Number of infected per capita, E
  - Deaths per infected, V
  - Deaths per nation, S
- OWID data confirms that the severity of the COVID-19 pandemic can be computed using $S=VEP$



PDFs for the COVID-19 pandemic. Solid lines with solid markers indicate empirical data, dotted lines with no markers indicate parametric fits to data, and the thick semi-transparent line indicates the curve computed using the relation $S=VEP$.

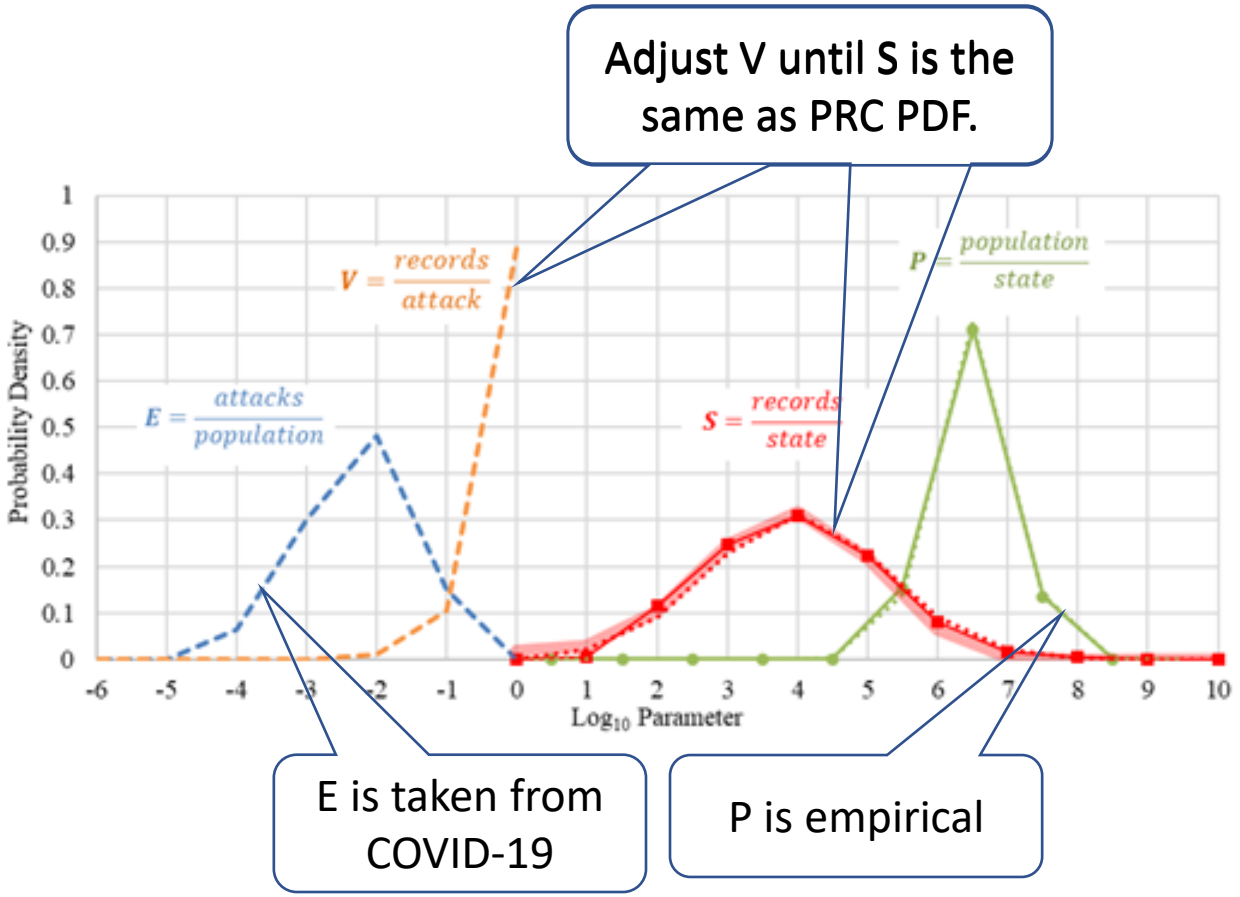
PDFs for War and COVID Compared

- Both phenomena may be decomposed according to $S=VEP$.
- Both exhibit similar trends (e.g., the same underlying parametric distributions)
- Hypothesize similar behavior for global cyber disaster.



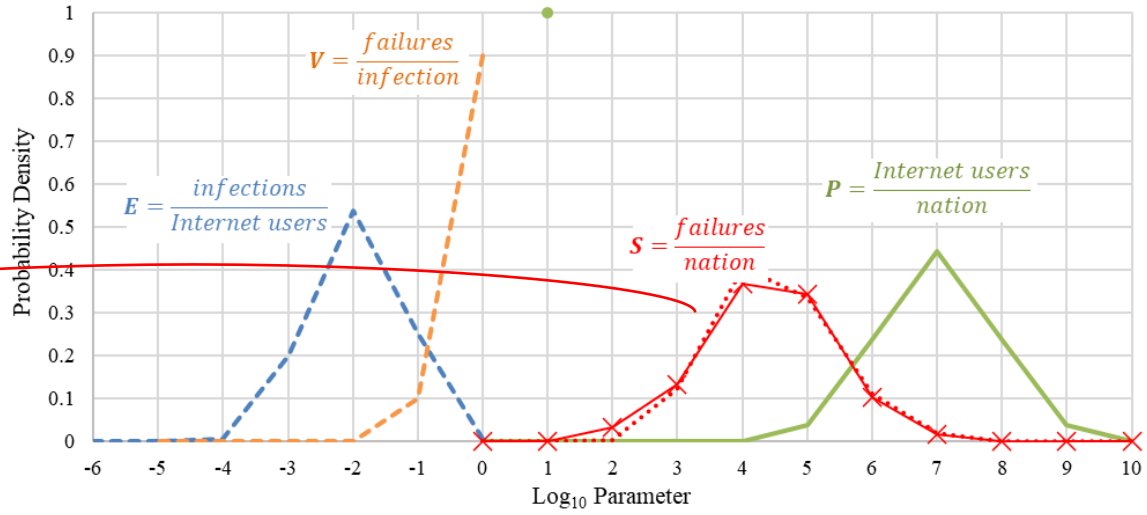
Estimate the PDF for a Global Cyber Disaster

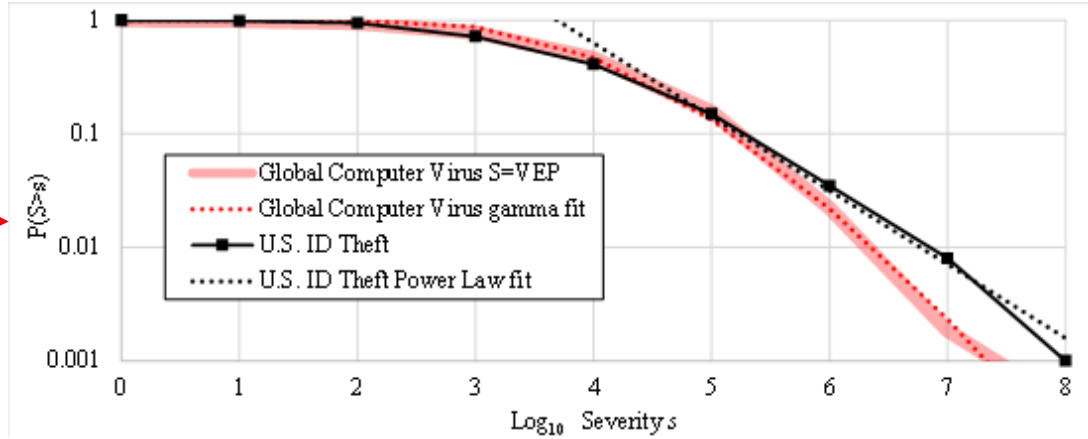
- There exists no public data that allows the determination of severity for a global computer virus.
- Use severity distribution obtained from the Privacy Rights Clearinghouse (PRC).
- Posit that the exposure distribution for a global computer virus is a network phenomena that mimics COVID.
- Adjust V until $S=VEP$ yields the distribution observed in the PRC data. This is the vulnerability of computers to the virus.
- Use "reverse-engineered" V to estimate cyber disaster with worldwide state population distribution P.



Cyber Disaster Exceedance Probability

$$P(S > s) = 1 - \int_0^s PDF\ ds$$





Parametric Fits to PDFs

Parametric distribution can be used in operational computer software designed to detect and react to cyber threats in real-time, in stochastic decision formulae enabling authorities to optimally choose among alternative cyber preparedness or resilience measures, or in actuarial equations to determine insurance premiums for cyber risks.

	Interstate War	Coronavirus Pandemic	Records Theft	Computer Virus
P	SLN ξ=8, ω=1.2, α=-3	SLN ξ=8.4, ω=1.5, α=-3	SLN ξ=7.8, ω=1.2, α=-2	SLN ξ=7, ω =0.9, α=0
E	LG α=17, β=0.13	LG α=14, β=0.20	LG α=14, β=0.20	LG α=14, β=0.20
V	LG α=1.0, β=2.0	LG α=5.5, β=0.35	LG α=1.0, β=0.50	LG α=1.0, β=0.50
S	LG α=9.8, β=0.34	LG α=4.0, β=0.6	LG μ=3.5, σ=1.3	LG α=4.0, β=0.6

Conclusion

We extend previous catastrophe theory that has been applied to interstate war to the coronavirus pandemic to develop a method for characterizing the magnitude and uncertainty of the severity S of a global computer virus that spreads to Internet-connected computers. The results are expected to help inform the development and implementation of cyber preparedness and resilience measures.