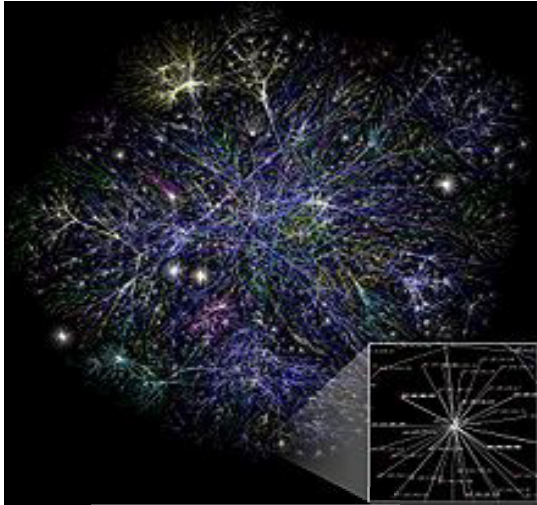


# ***Towards Reliability/Security Risk Metrics for Large-Scale Networked Infrastructures: Work in Progress***

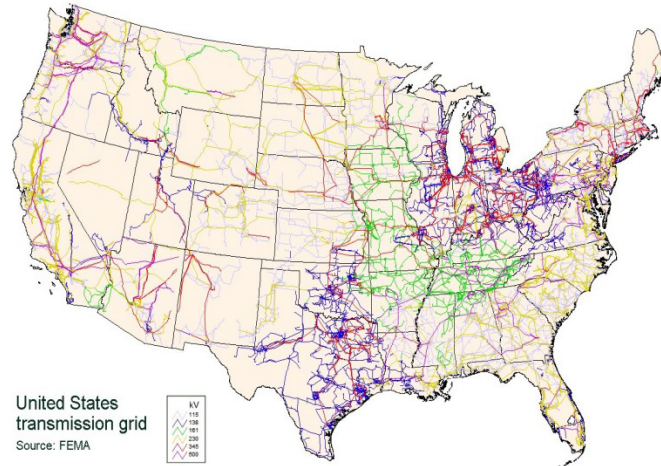
**Vladimir Marbukh, NIST**

**PSAM 2022**

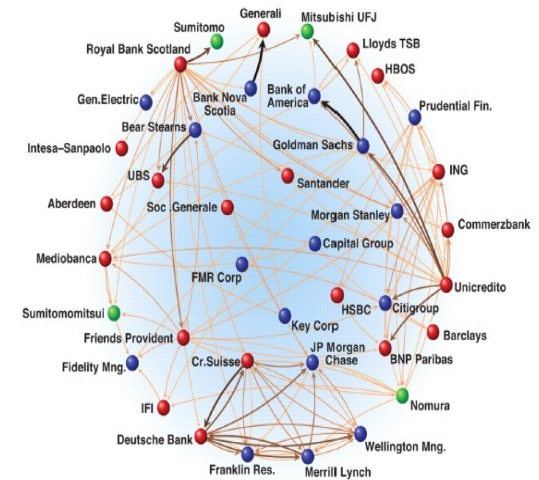
# Large-Scale Networked Infrastructures: Phenomenology



**The Internet**



**The Power Grid**



**The Financial Network**

## Inherent connectivity systemic benefit/risk tradeoff

Connectivity is economically driven (rich gets richer, economy of scale, risk sharing, etc.)  
 Economics fail to address systemic risks of: (cyber)security, cascading failures, etc.

**Conventional Risk Management:** use historical data to extrapolate, i.e., “fight the last war”.

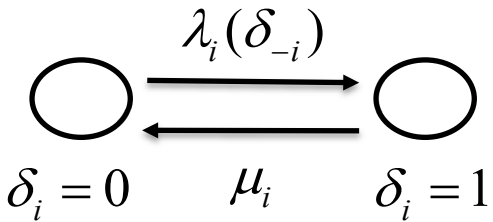
**Challenge:** unexpected consequences due to

- externalities due to strategic selfish or malicious (cybersecurity, terrorism) components
- non-linear component interactions, randomness, e.g., stochastic resonance

**Ultimate Goal:** systemic risk/benefit control through combination of regulations/incentives

# Markov Dynamics => Markov Random Field

Failure dynamics is described by a homogeneous in time Markov process with locally interacting components.

$$\delta(t) = (\delta_1(t), \dots, \delta_N(t)) \in \{0, 1\}^N$$


$$\lambda_n(\delta_{-n}) = \lambda_n(\delta_k : A_{kn} = 1) \quad \text{where}$$

$$A = (A_{kn})_{k,n=1}^N \quad \text{incidence matrix of directed graph G describing contagion}$$

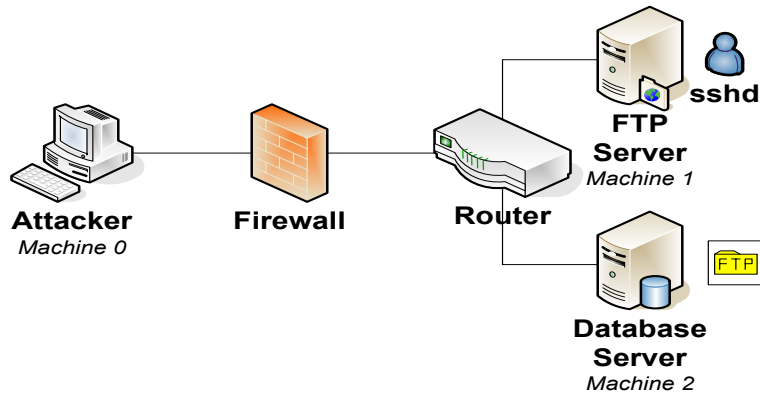
$$\text{Markov random field: } p_n(\delta_n | \delta_{-n}) = p_n(\delta_n | \delta_k : A_{kn} = 1)$$

$$\text{Approximation: } P(\delta) \approx Z^{-1} \prod_{n=1}^N p_n(\delta_n | \delta_{-n}), \quad Z = \sum_{\delta \in \{0,1\}^N} \prod_{n=1}^N p_n(\delta_n | \delta_{-n})$$

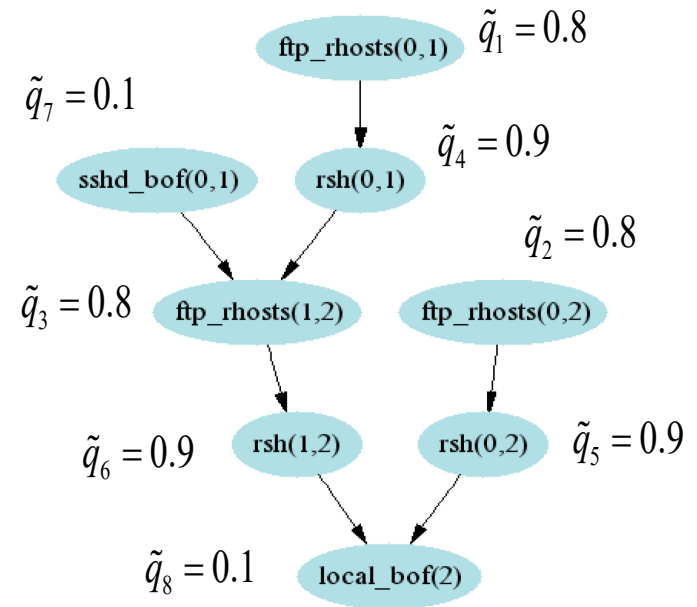
$$\text{Example: } p_n(\delta_n | \delta_{-n}) = \begin{cases} q_n[\gamma_n + (1 - \gamma_n)\chi_n(\delta_{-n})] & \text{if } \delta_n = 1 \\ 1 - q_n[\gamma_n + (1 - \gamma_n)\chi_n(\delta_{-n})] & \text{if } \delta_n = 0 \end{cases}$$

Acyclic graph G defines Bayesian network, e.g., Bayesian Attack Graph (BAG)

# Bayesian/Probabilistic Attack Graph



The attack graph depicts three attack paths. On the right, the attack path starts with a ssh buffer overflow exploit from machine 0 to machine 1, which gives the attacker the capability of executing arbitrary codes on machine 1 as a normal user. The attacker then exploits the ftp vulnerability on machine 2 to anonymously upload a list of trusted hosts. Such a trust relationship enables the attacker to remotely execute shell commands on machine 2 without providing a password. Consequently, a local buffer overflow exploit on machine 2 escalates the attacker's privilege to be the root of that machine. Details of the other two attack paths are similar.



ftp-rhosts(0,1)=v1,  
 ftp-rhosts(0,1)=v2,  
 ftp-rhosts(1,2)=v5,  
 rsh(0,1)=v4,  
 rsh(0,2)=v5,  
 rsh(1,2)=v6,  
 sshd\_bof(0,1)=v7,  
 local\_bof(2)=v8.

## Security Risk Metrics

Analytical representation of Attack Graph (AG):  $\delta_n = \sigma_n \chi_n(\delta_{-n})$

Due to acyclic AG, this system has unique solution:  $\delta_n = \sigma_n \varphi_n(\sigma_{-n})$

System loss function:  $L(\delta)$ . Average loss:

$$L^{ave} := E_p[L(\delta)] = E_{\tilde{Q}}[L(\sigma)] = \sum_{\sigma \in \{0,1\}^N} L(\sigma) \prod_n \tilde{q}_n^{\sigma_n} (1 - \tilde{q}_n)^{1 - \sigma_n}$$

where renormalized system loss function:  $L(\sigma) := L[\sigma_1 \varphi_1(\sigma_{-1}), \dots, \sigma_N \varphi_N(\sigma_{-N})]$

In example:  $L^{ave} = L\tilde{p}_8 \approx 0.087L$  since  $L(\sigma) = \sigma_{-8} \varphi_8(\sigma_{-8})$ ,

$$\varphi_8(\sigma_{-8}) = \sigma_2 \sigma_5 + (1 - \sigma_2 \sigma_5)(\sigma_1 \sigma_4 + \sigma_7 - \sigma_1 \sigma_4 \sigma_7) \sigma_3 \sigma_6$$

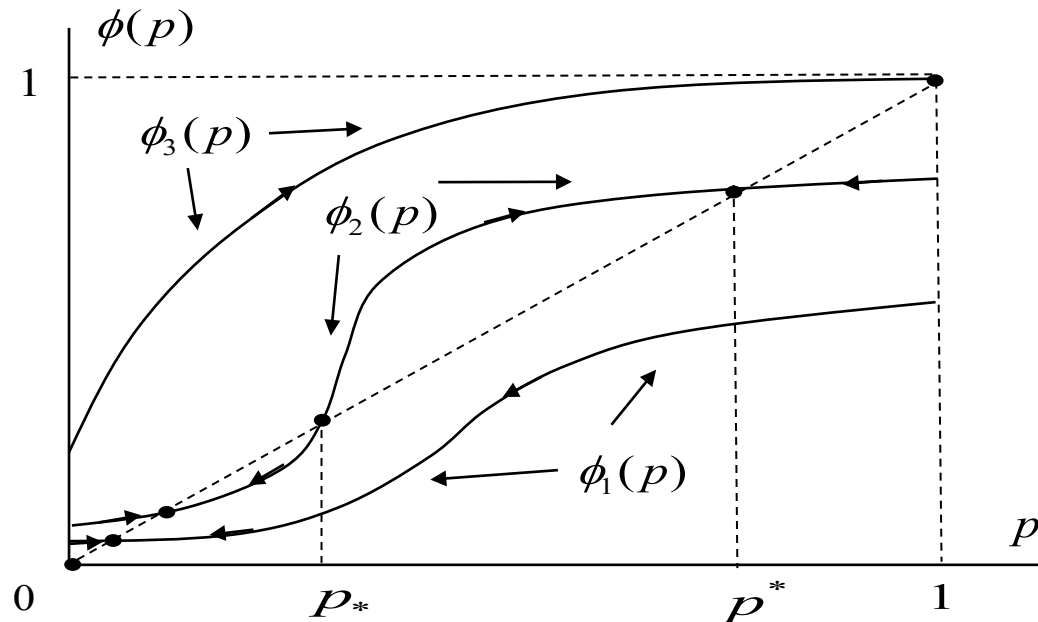
**Conclusions** (good and bad news):

- Can be extended to modern risk metrics, e.g., CyVaR, CyCVaR, CyEVar
- Analysis of acyclic AG, if not very large, is computationally feasible
- Acyclic AG does not describe cascading failures

## Markov Field with Cycles

$$\text{Model: } p_n(\delta_n | \delta_{-n}) = \begin{cases} q[\gamma + (1-\gamma)\chi_n(\delta_{-n})] & \text{if } \delta_n = 1 \\ 1 - q[\gamma + (1-\gamma)\chi_n(\delta_{-n})] & \text{if } \delta_n = 0 \end{cases}$$

Mean-field approximation in homogeneous case:  $p = q\phi(p)$



Bi-stability indicates a possibility of cascading failures

## Onset of Cascading Failure

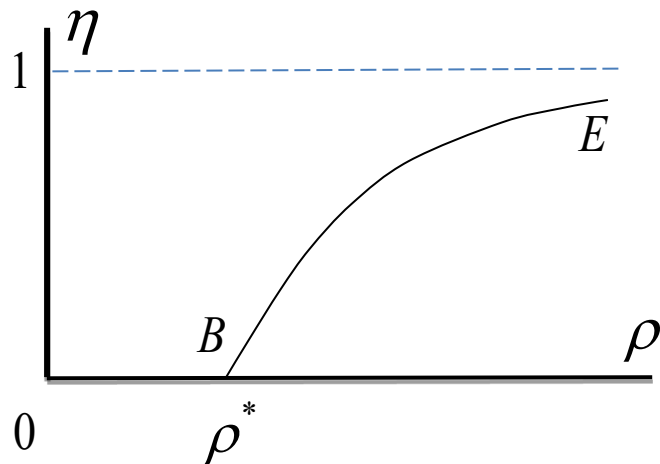
Since we are interested in contagion emergence, consider expansion of contagion rate

$$\lambda_i(\delta_{-i}) = \sum_{j \in \mathbf{J}_i} \lambda_{ij} \delta_j + \sum_{j, j \in \mathbf{J}_i} \delta_j \sum_{k, k \in \mathbf{J}_j \setminus i} \lambda_{ijk} \delta_k + \dots$$

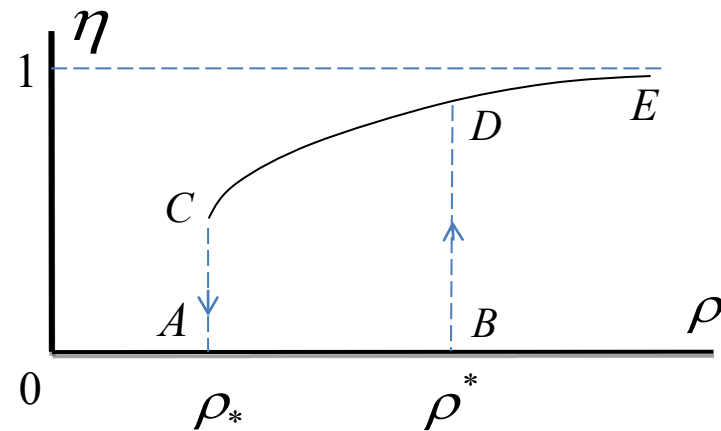
It is known [2] that contagion-free region is given by condition is  $\gamma < 1$

Here  $\gamma$  is Perron-Frobenius eigenvalue of matrix  $\mathbf{B} = (\beta_{ij})_{i,j=1}^N$ ,  $\beta_{ij} = \lambda_{ij} / \mu_j$

Order parameter is portion of system affected by contagion:  $\eta = N^{-1} \sum_{i=1}^N \delta_i$



Continuous failure



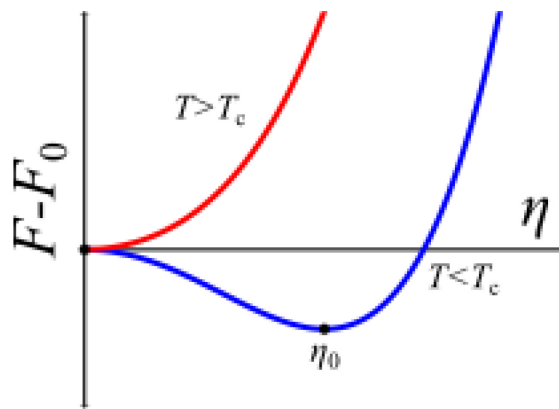
Discontinuous failure

# Landau Theory of Phase Transitions

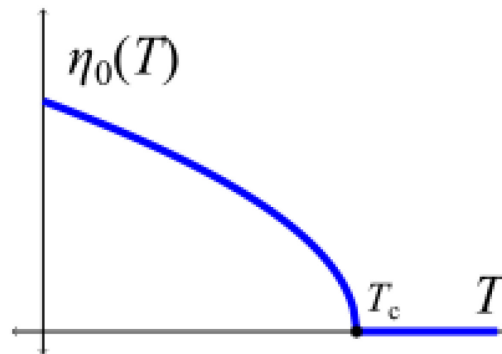
Probability density of order parameter  $p(\eta) \sim e^{-F(T,\eta)/\varepsilon}$

Given temperature  $T$ , order parameter  $\eta$  minimizes free energy  $F(T, \eta)$

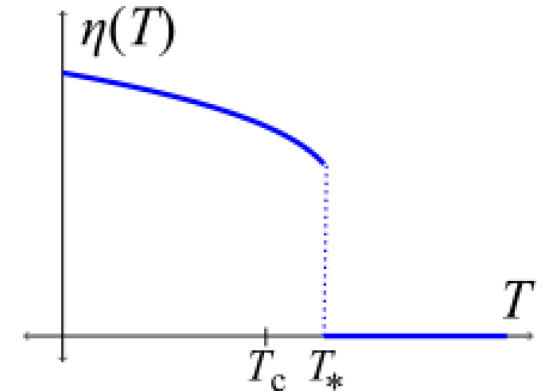
Free energy is analytic function



Free energy vs. order parameter



Second order (continuous) phase transition



First order (discontinuous) phase transition

**Landau theory of phase transitions** [Lev D. Landau, 1937]:

- Is a phenomenological (mean-field) approximation
- Gives a qualitative, and in some cases, quantitative description
- Closely related to Catastrophe Theory [René Thom, 1960s]



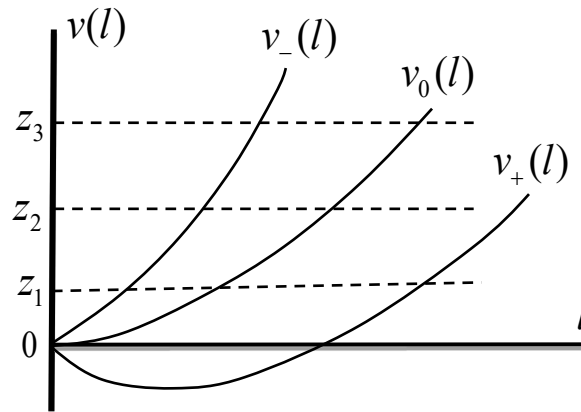
# Landau Potential at Onset of Systemic Failure

Dimension reduction in a proximity at onset of systemic failure is due to critical slowdown, i.e., order parameter evolves on much slower time scale than the rest of dynamic variables. This allows us to approximate the evolution of order parameter by a Markov birth-death process, and in particular write steady-state distribution of order parameter in potential form. [V. Marbukh, NetSciX 2022].

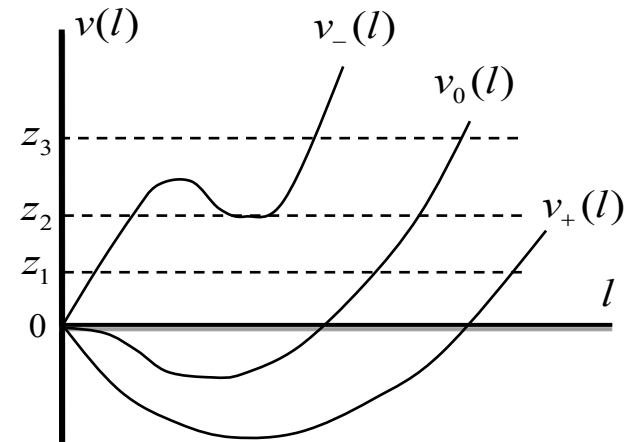
If contagious node experiences loss, the steady-state distribution of aggregate normalized loss can be written in potential form:

$$p(l) \sim e^{-Nv(l)}$$

Potential  $v(l)$  inside, on the boundary, and outside of the contagion-free region



Continuous



Discontinuous

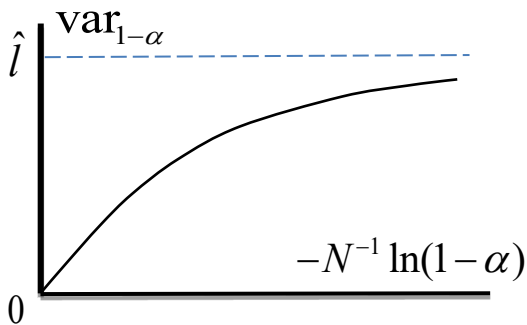
Landau potential for normalized aggregate losses

## Risk of Systemic Failure

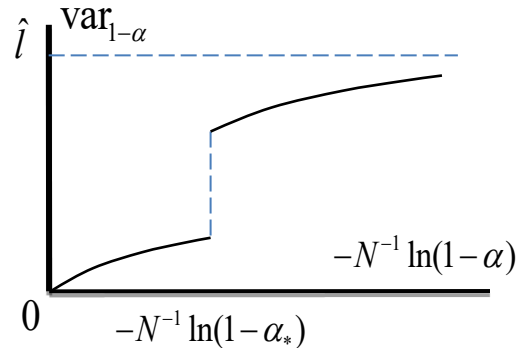
Normalized value at risk  $\text{var}_{1-\alpha} = N^{-1}VaR_{1-\alpha} = \arg \min_{l \geq 0} v(l)$

subject to  $v(l) \geq -N^{-1} \ln(1-\alpha)$  since  $p(l) \sim e^{-Nv(l)}$

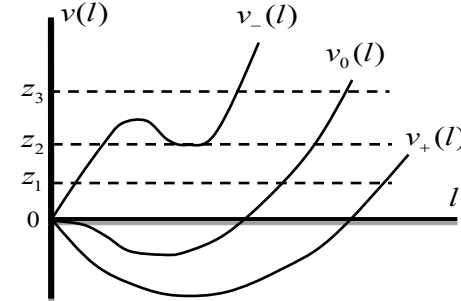
Parameter  $0 \leq \alpha < 1$  characterizes decision maker risk averseness



a. Continuous



b. Discontinuous



Normalized var vs. risk averseness inside contagion-free region

This approach quantifies risk of undesirable contagion inside contagion-free region, which accounts for risk averseness and continuous/discontinuous contagion emergence, e.g., discontinuity in (b) occurs at the point  $-N^{-1} \ln(1-\alpha_*) = z_2$

Also, this approach yields mapping from risk averseness to “safety margin” in terms of distance from the boundary of the contagion-free region.

# *Conclusions & Future Research*

## **Conclusions:**

- Since systemic instabilities are unavoidable, system designers/operators should take into account systemic risk
- Since cascading failure is in effect a collective phenomenon, we propose systemic risk metrics based on Landau theory of phase transition.
- These metrics distinguish between more dangerous abrupt/discontinuous and less dangerous gradual/continuous instabilities.

## **Future research:**

- Verification/validation mean-field approximation through simulations, measurements and rigorous analysis (doubtful).
- Possibility of online measurement of the P-F eigenvalue as a basis for “early warning system.”
- Possibility of controlling Networked Systems through a combination of regulations and pricing, based on the P-F eigenvalue.

***Thank you!***