



HISOLUTIONS

Assume Trauma

Resilienz und Coping-Mechanismen bei kritischen Infrastrukturen



David Fuhr

@0xdhf

isher of puns
curious curer of se
searcher of re @hisolutions
he/his/him

And I mentor. I meant OR.

A small green seedling with two leaves is growing out of a vast, flat, orange-red desert landscape. The background is a blurred view of a desert valley with some greenery in the distance under a blue sky with light clouds.

Trauma

Resilienz

&

Coping-Mechanismen

in KRITIS



Wie ein Pfeil fliegt man daher – als ob man selber einer wär. – Anonyme Schiffsschaukel



Trau·ma

/Traûma/

Substantiv, Neutrum [das]

1. MEDIZIN • PSYCHOLOGIE
starke psychische Erschütterung, die [im Unterbewusstsein] noch lange wirksam ist
"ein Trauma haben, erleiden"
2. MEDIZIN
durch Gewalteinwirkung entstandene Verletzung des Organismus





Resilienz (Psychologie)

Resilienz (von **lateinisch** *resilire* ‚zurückspringen‘ ‚abprallen‘) oder **psychische Widerstandsfähigkeit** ist die Fähigkeit, Krisen zu bewältigen und sie durch Rückgriff auf persönliche und sozial vermittelte Ressourcen als Anlass für Entwicklungen zu nutzen.

Resilienz (von lateinisch *resilire* „zurückspringen, abprallen“) steht für:

- **Resilienz (Ingenieurwissenschaften)**, Fähigkeit von technischen Systemen, bei einem Teilausfall nicht vollständig zu versagen
- **Resilienz (Energiewirtschaft)**, Ausfallsicherheit in der Energieversorgung
- **Resilienz (Ökosystem)**, Fähigkeit eines Ökosystems, nach einer Störung zum Ausgangszustand zurückzukehren
- **Resilienz (Psychologie)**, psychische Widerstandsfähigkeit
- **Resilienz (Soziologie)**, Fähigkeit von Gesellschaften, externe Störungen zu verkraften
- **Resilienz (Zahnmedizin)**, Nachgiebigkeit der Mundschleimhaut bei Belastung
- **Resilienz**, systemische Widerstandsfähigkeit von Unternehmen gegenüber Störungen, siehe **Resilienz-Management**

Siehe auch:

- organisatorische Resilienz (BSI-Standard)
- Fehlertoleranz (Resilienz technischer Systeme)

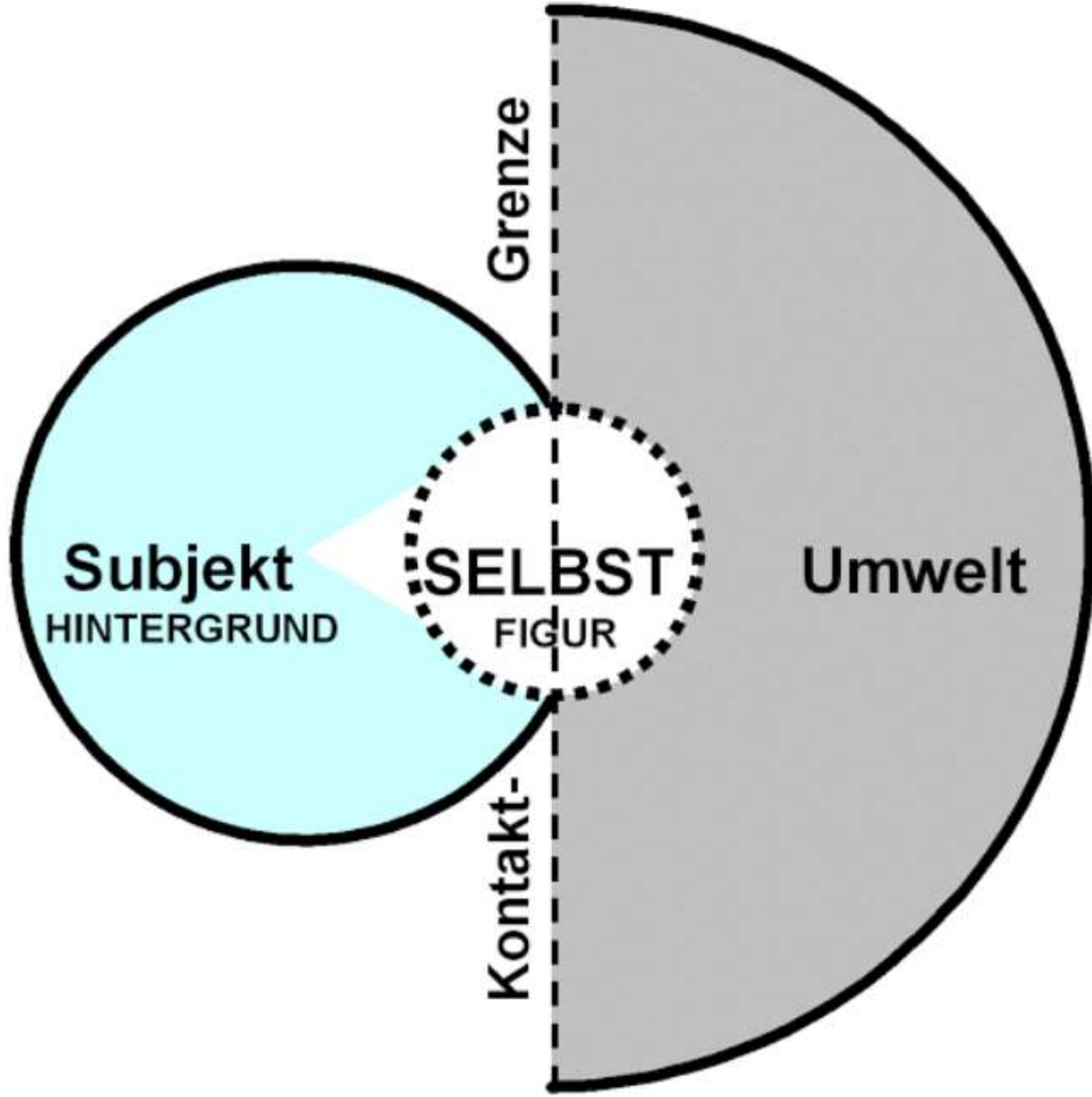


Bewältigungsstrategie

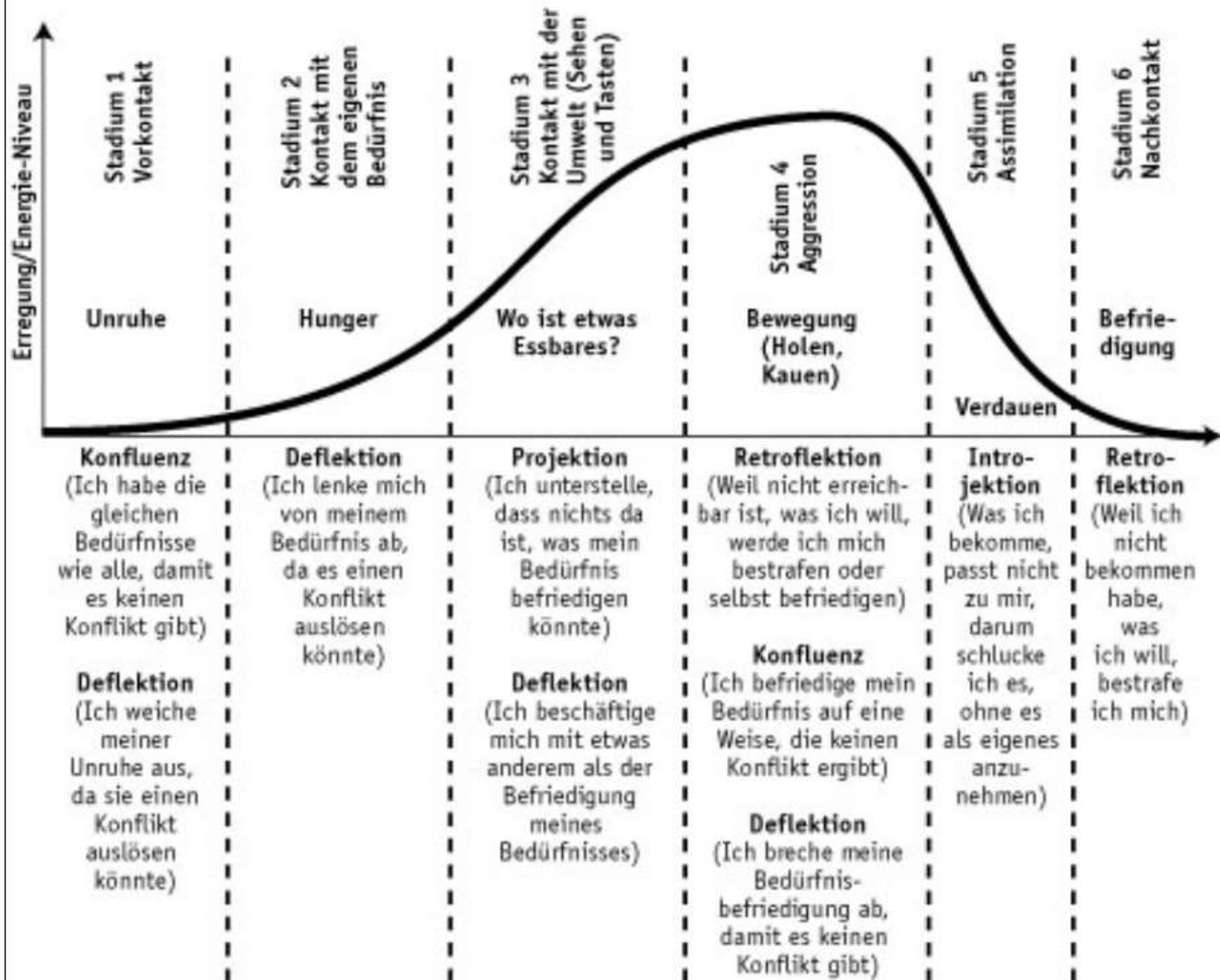
Die Begriffe **Bewältigungsstrategie**, **Copingstrategie** oder **Coping** (von englisch *to cope with*, „bewältigen, überwinden“) bezeichnen die Art des Umgangs mit einem als bedeutsam und schwierig empfundenen Lebensereignis oder einer Lebensphase.



Modelle der Seele



Die Kontaktstörungen



Umwelt

Reize (Stressoren)

WahrnehmungsfILTER (Selektion)

Person

Primäre Bewertung

Interpretation des Stressors

positiv

gefährlich

*Herausforderung,
Bedrohung,
Verlust*

irrelevant

Sekundäre Bewertung

Analyse der verfügbaren Ressourcen

mangelnde
Ressourcen

ausreichende
Ressourcen

Stress

Coping

Stressbewältigung

problemorientiert

Situation selbst ändern

emotionsorientiert

Bezug zur Situation ändern

Neubewertung

Anpassung und Lernen

Richard S. Lazarus (* 3. März 1922 in New York; † 24. November 2002 in Walnut Creek) war ein amerikanischer Psychologe und führender Verfechter der Emotionstheorie der kognitiven Bewertung.^[1] Er entwickelte eine Theorie zur Stressbewältigung, die als Stressmodell von Lazarus seinen Namen trägt, und leistete Beiträge zur Kognitiven Wende.





Konzepte

Prospect
Theory

Antifragilität

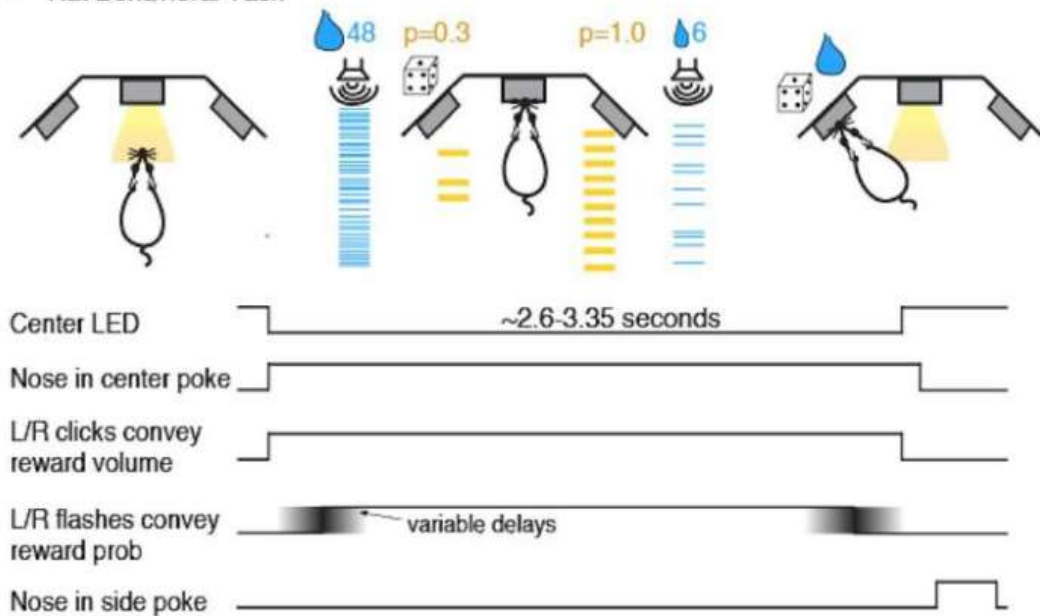
Resilienz
(faktoren)

Chaos
Engineering

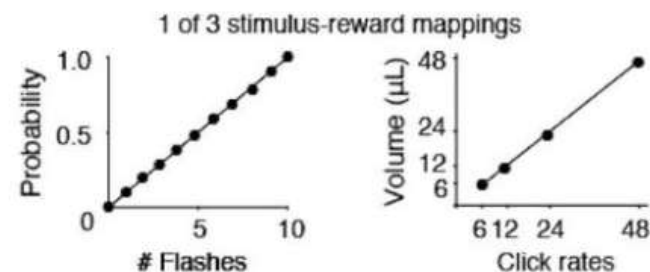


Prospect Theory

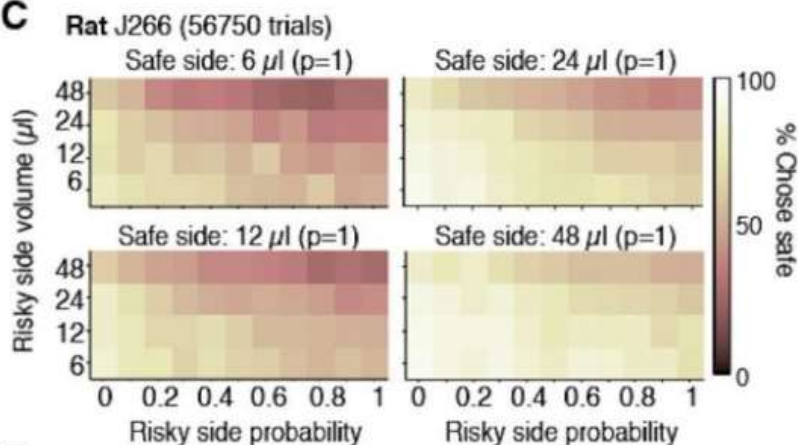
A Rat Behavioral Task



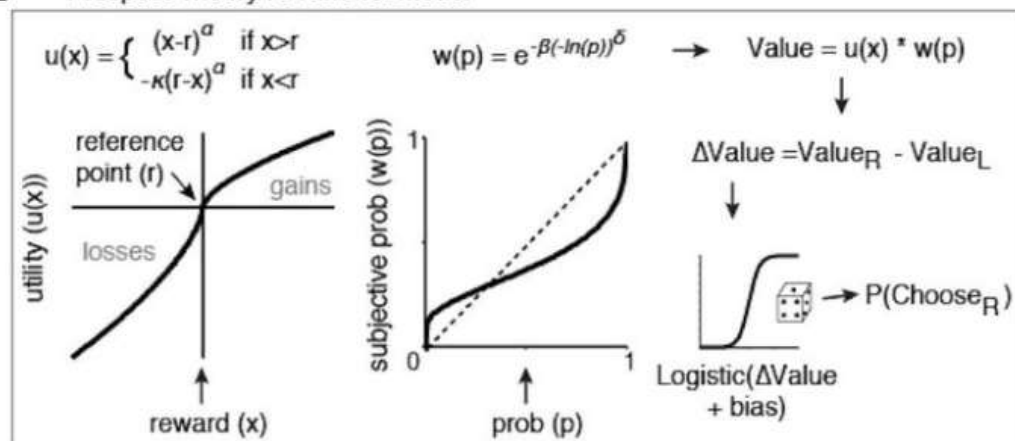
B



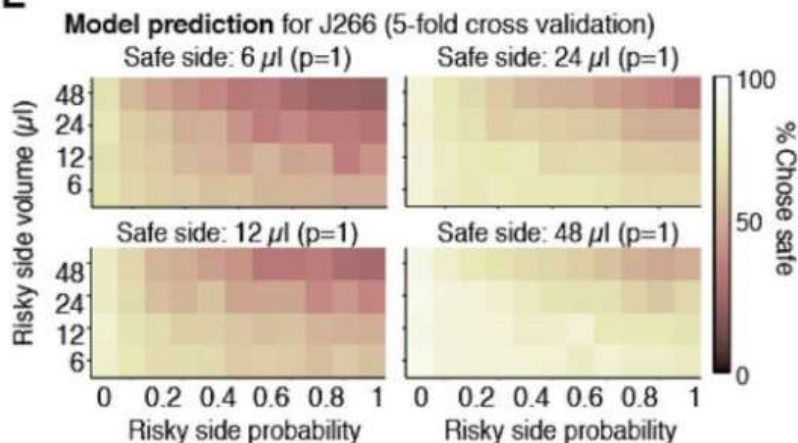
C

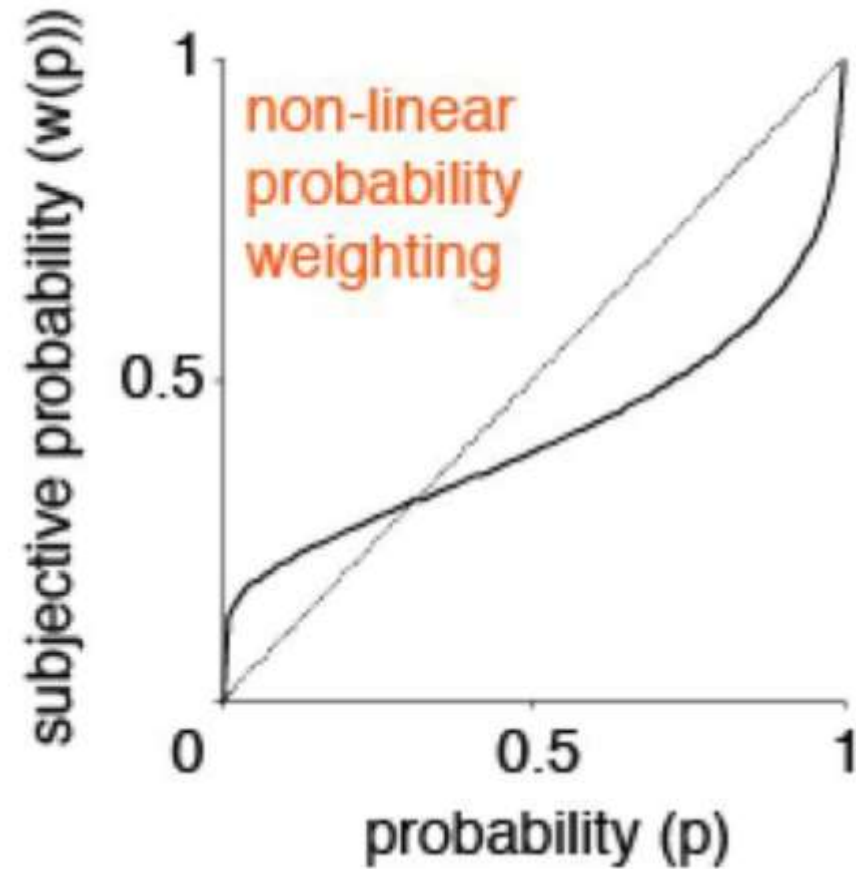
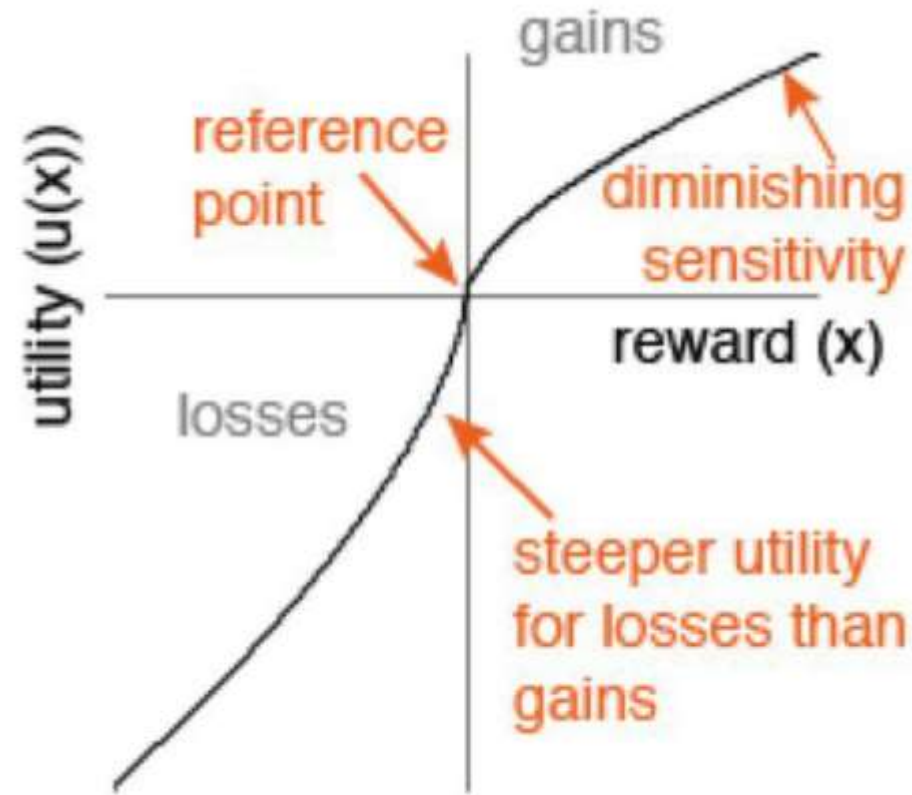


D Prospect Theory Behavioral Model



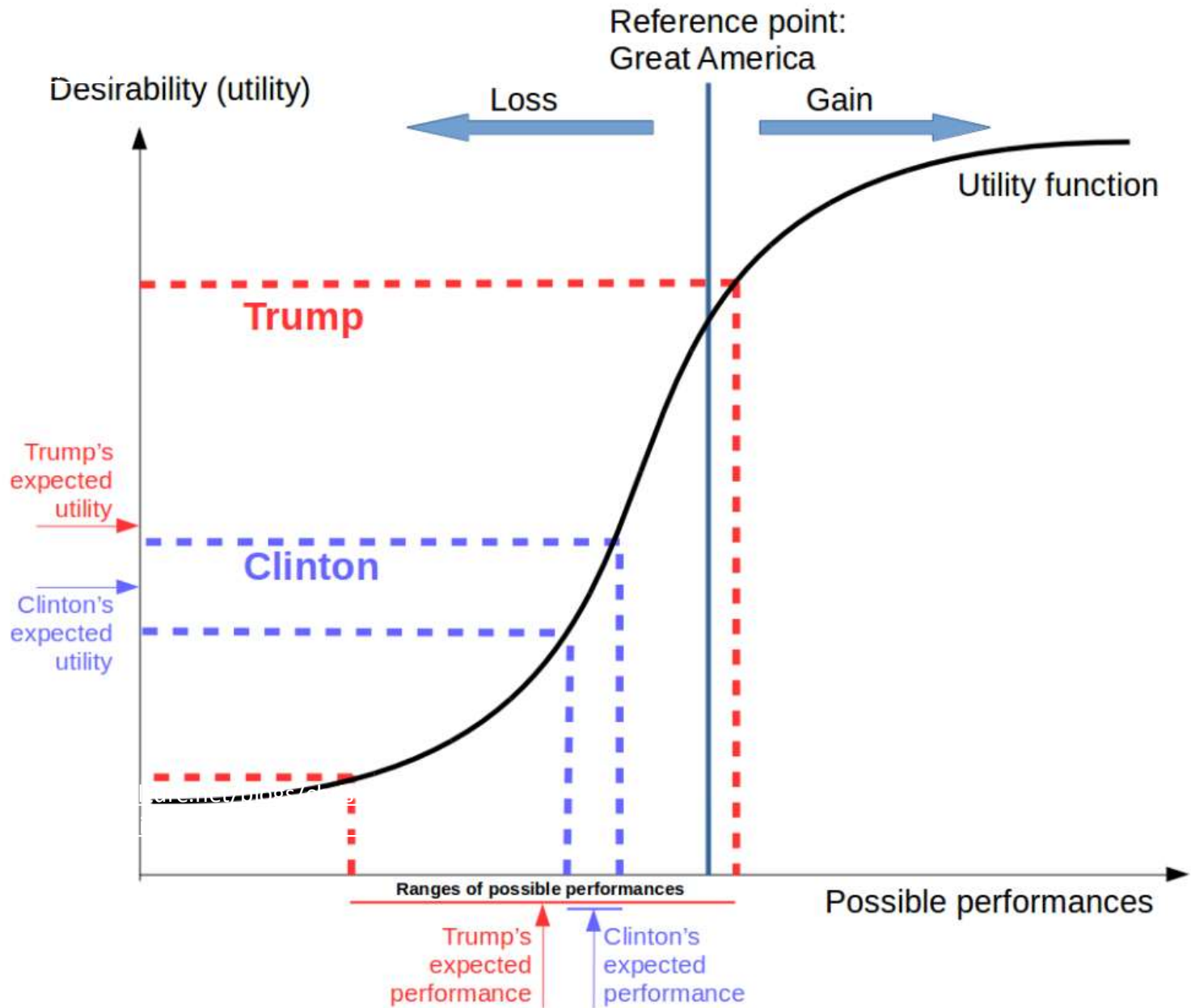
E





Prospect Theory framework

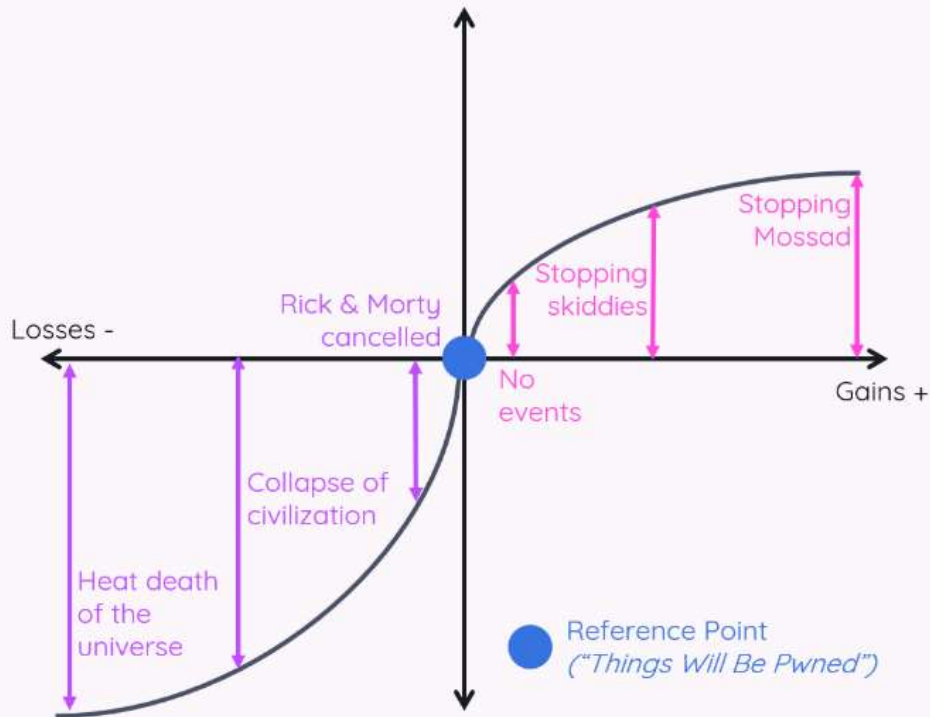
- (1) diminishing marginal sensitivity
- (2) loss aversion (utility function is steeper for losses than gains)
- (3) reference dependence (rewards evaluated relative to a reference point)
- (4) probability distortion, or nonlinear probability weighting.



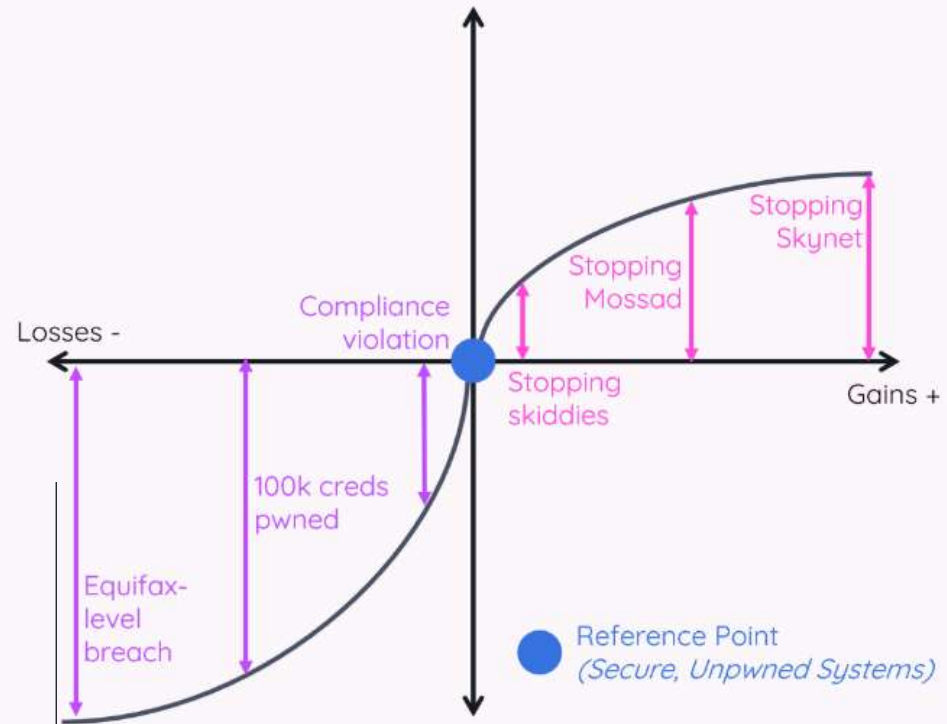


Kelly Shortridge
VP Product Strategy
Capsule8

Prospect Theory Graph:
Enterprise Information Security + Chaos

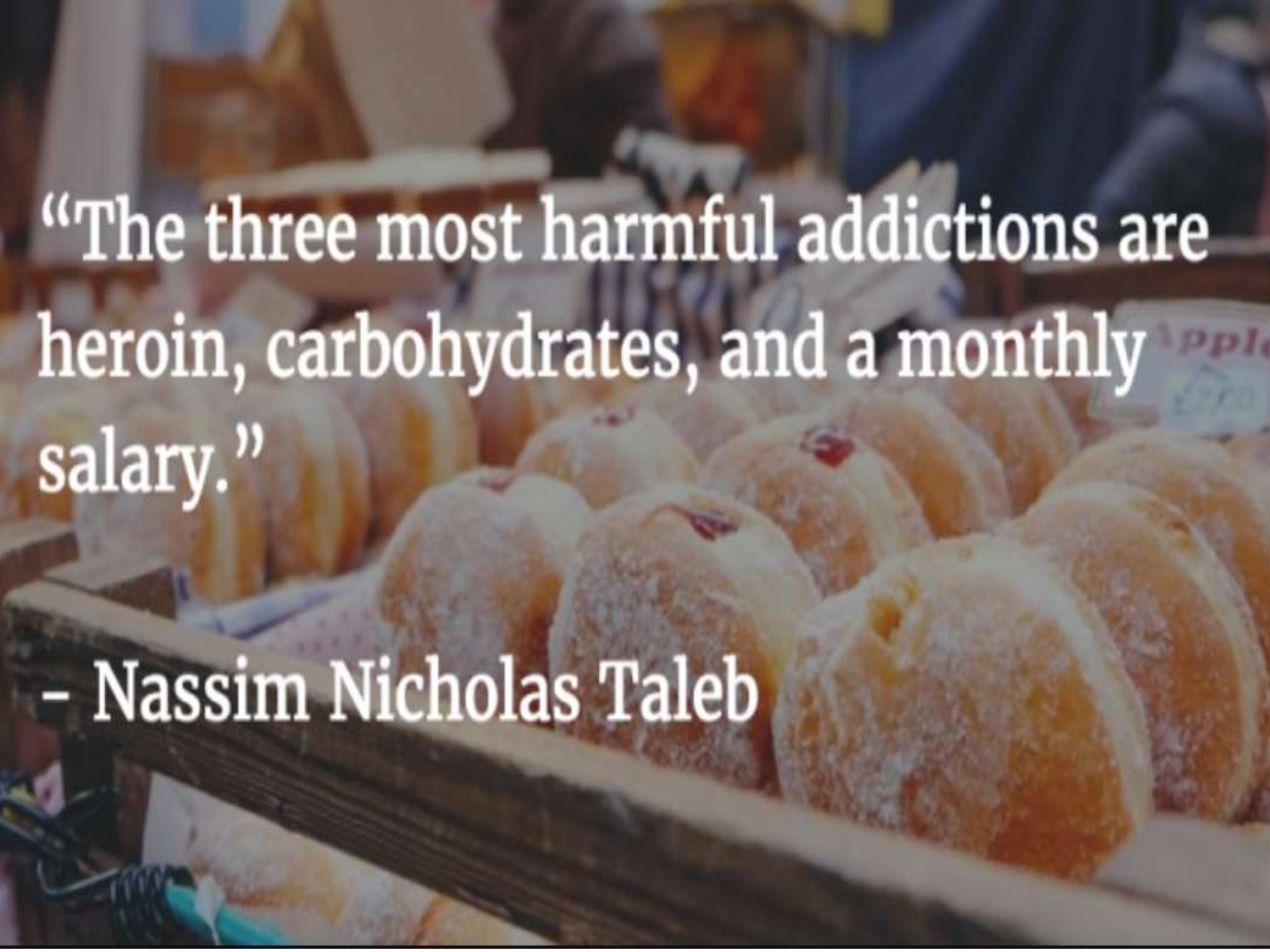


Prospect Theory Graph:
Enterprise Information Security Today



A close-up photograph of a white rabbit being held gently by a human hand. The rabbit has long, upright ears and is looking directly at the camera. A red and white 'FRAGILE' label is placed over the lower left portion of the rabbit's face and the hand holding it. The background is blurred, showing what appears to be a wooden fence or structure.

FRAGILE
HANDLE WITH CARE



“The three most harmful addictions are
heroin, carbohydrates, and a monthly
salary.”

– Nassim Nicholas Taleb

Nassim Nicholas Taleb

ANTIFRAGILE

THINGS THAT GAIN FROM DISORDER

New York Times BESTSELLER

AUTHOR OF *The Black Swan*

"Startling... richly crammed with insights, stories, fine phrases and intriguing asides... I will have to read it again. And again."

—Matt Ridley, *THE WALL STREET JOURNAL*

Fragile



- Suffers or breaks from volatility
- More downside than upside from volatility
- Seeks tranquility
- Mistakes rare and large
- Myth: Sword of Damocles

Resilient



- Stays the same in volatility
- Indifferent to tranquility and volatility
- Myth: The Phoenix

Antifragile



- Grows and gets stronger from volatility
- More upside than downside from volatility
- Seeks disorder
- Mistakes small and benign
- Myth: The Hydra

The Art of
MANLINESS
EST. 2009

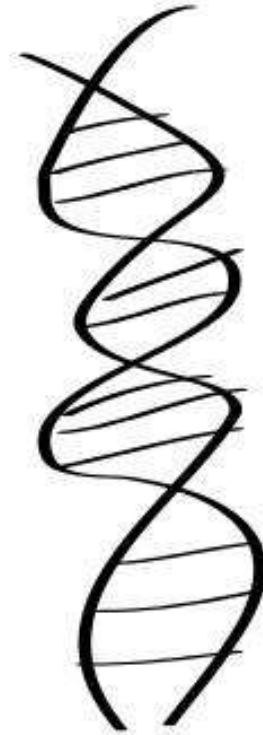
Fragile



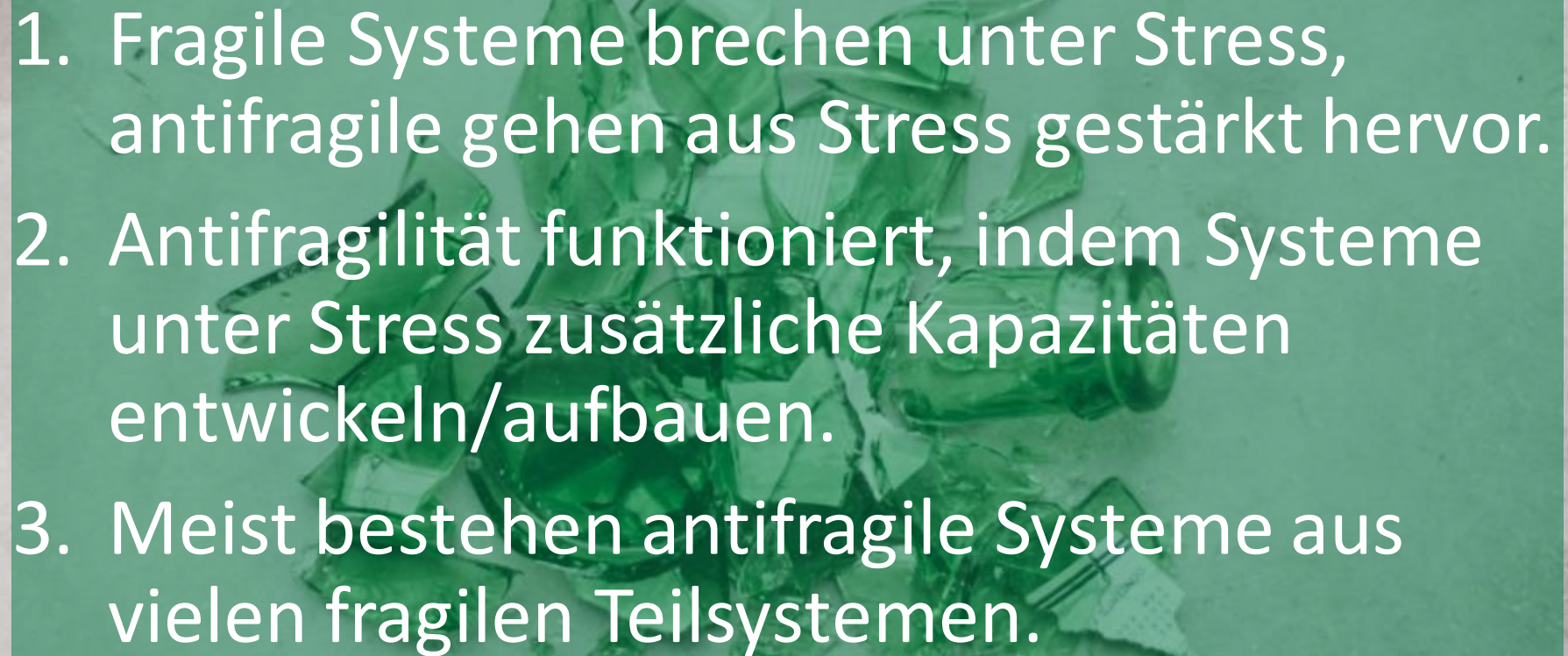
Robust



Anti-Fragile

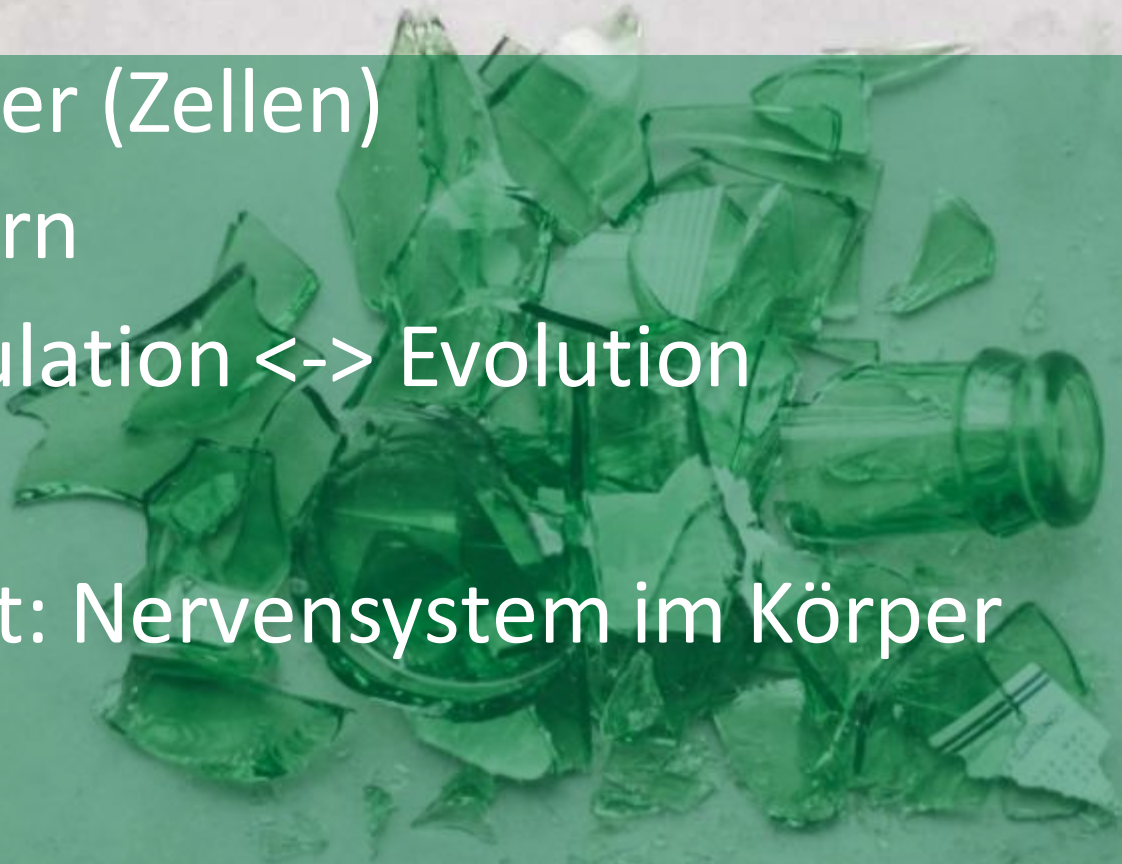


Antifragilität

- 
1. Fragile Systeme brechen unter Stress, antifragile gehen aus Stress gestärkt hervor.
 2. Antifragilität funktioniert, indem Systeme unter Stress zusätzliche Kapazitäten entwickeln/aufbauen.
 3. Meist bestehen antifragile Systeme aus vielen fragilen Teilsystemen.

Antifragilität

- Körper (Zellen)
- Gehirn
- Population $\leftrightarrow$ Evolution
- Nicht: Nervensystem im Körper





Bewältigung (Coping)

(Innere) Resilienzfaktoren

1. Akzeptanz: Krisen als Teil des Lebens annehmen
2. Optimismus: positive Perspektive
3. Selbstwirksamkeit: Glaube an eigene Fähigkeiten und Kompetenzen
4. Eigenverantwortung: Bemühen, jegliche Probleme eigenverantwortlich zu lösen, auch wenn nicht selbst verursacht
5. Netzwerkorientierung: soziale Beziehungen und die Fähigkeit, Unterstützung in Krisen annehmen zu können
6. Lösungsorientierung: sich offenbarende Wege nutzen, gestärkter hervorzugehen und zu lernen

Resilienzfaktoren KRITIS

1. Akzeptanz:

- i. Assume Breach (aber siehe 2.)
- ii. Krisen als Teil des Betriebs annehmen -> planen und üben

2. Optimismus -> Awareness

3. Selbstwirksamkeit: Entwicklung eigener Fähigkeiten und Kompetenzen → Bildung / Schulung / Training (zentral)

4. Eigenverantwortung: Probleme eigenverantwortlich lösen, auch wenn nicht selbst verursacht

- i. MIRT?
- ii. Ökonomische und regulatorische Anreize?
- iii. (Temporäre) (Wieder-)Verstaatlichung?

Resilienzfaktoren KRITIS

5. Netzwerkorientierung: Beziehungen fördern zwischen

- i. Individuen, Betreibern, Industrie, Staat, Community
- ii. Unterstützung in Krisen
 - i. annehmen zu können
 - i. erlauben
 - ii. fördern / fordern
 - ii. geben zu können
 - i. erleichtern
 - ii. fördern / fordern



6. Lösungsorientierung: Lernen aus

- i. Vorfällen: eigenen, national, international
- ii. Near Misses
- iii. „Melde“, „pflicht“ → (nachdrückliche) „Austausch“, „einladung“

Chaos Engineering





Choose a Gremlin

Select the type of attack to unleash.

1 ↺ ↻ ⋮

Contact sales to upgrade and unlock all attacks.

Category



Resource

Impact cores, workers, and memory



State

Process killer, shutdown and time travel.



Network

Blackhole, latency, packet loss and DNS

Attacks



Process Killer

An attack which kills the specified process



Shutdown

Reboots or shuts down the targeted host operating system



Time Travel

Changes the system time

Delay

The number of minutes to delay before shutting down

1

Reboot

Indicates the host should reboot after shutting down

On



Run the attack

Unleash now or schedule for later.

Once on Mon, Wed, Thu from 11:00 to 15:00

⋮

Schedule for later

Run this attack at a future date

On



Only once

Set the date and time.



Randomly within a timeframe

Select at least one day.



Executions

The number of attacks per day

1

From

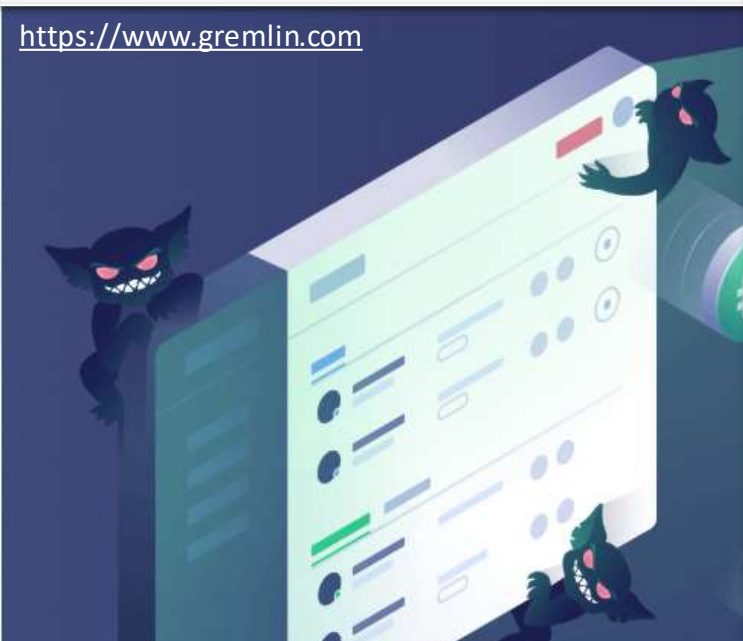
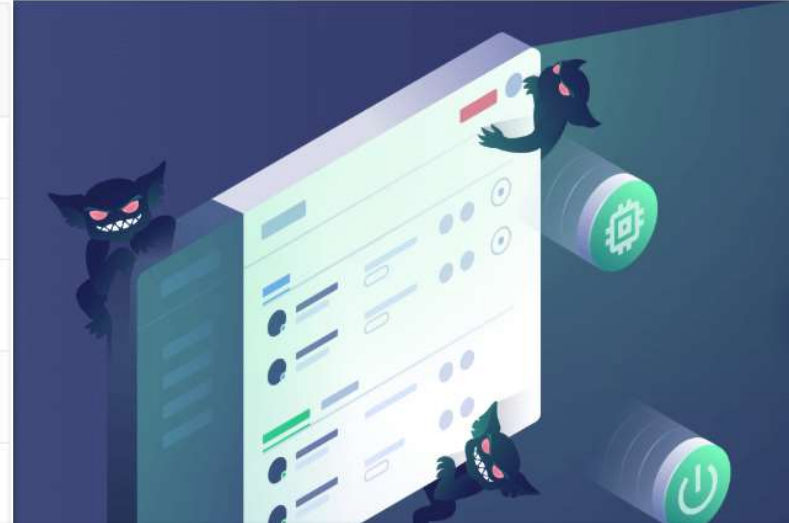
Local Military Time

11:00

To

Local Military Time

15:00



<https://www.gremlin.com>

Chaos Engineering

Like a vaccine, we inject harm
to build *immunity*.





Going There, Doing That

Chaotic Whoops: NotPetya@Maersk 2018

After a frantic global search, the admins finally found one lone surviving domain controller in a remote office—in Ghana.

known copy of the company's domain controller data left untouched by the malware—all thanks to a power outage. "There were a lot of joyous whoops in the office when we found it," a Maersk administrator says.

After a frantic search that entailed calling hundreds of IT admins in data centers around the world, Maersk's desperate administrators finally found one lone surviving domain controller in a remote office—in Ghana. At some point before NotPetya struck, a blackout had knocked the Ghanaian machine offline, and the computer remained disconnected from the network. It thus contained the singular

„Dumb Down“

Securing Energy Infrastructure Act (SEIA) (2019): 2y pilot program [...] to research and test solutions, including "analog and non-digital control systems."



Lessons To Be Learned... @Regulierung

- Tschernobyl-Trauma
 - No too big to fail
 - (Problem: Grid)
- Prospect Theory
 - Compliance reduzieren
 - Praktisches Notfall- und Krisenmanagement stärken
 - Anreize für Resilienz setzen (z. B. BNetzA)
- Chaos Engineering
 - Hilft ;-)
 - Skala designen und hochfahren



A detailed black and white illustration of a Komodo dragon, shown in a crawling posture. The dragon's body is covered in intricate scales, and its long tail extends across the frame. It is positioned above a blue rectangular area that contains the title text.

Site Reliability Engineering

HOW GOOGLE RUNS PRODUCTION SYSTEMS



Anlagen Resilience

Engineering

HOW NEULAND RUNS KRITIS SYSTEMS



HiSOLUTIONS

Fragen? Anregungen? Ideen?

David Fuhr
Head of Research, HiSolutions AG
fuhr@hisolutions.com

<https://research.hisolutions.com>

<https://twitter.com/0xdhf>