Open Universiteit

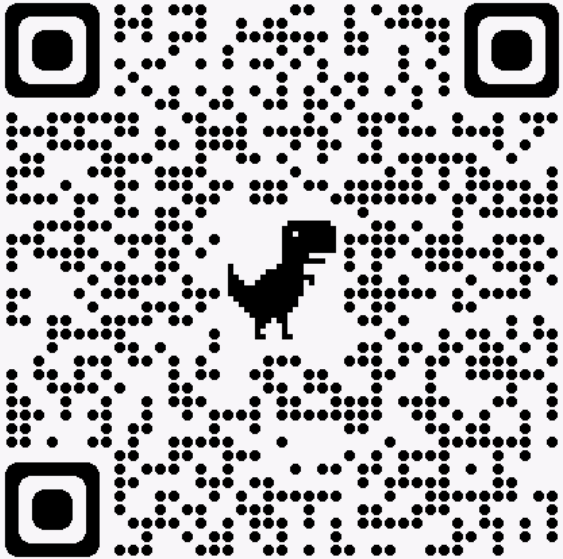
Cyber Resilience
By Edzo Botjes

PhD work group meeting Digital Security
@ ACademic Cyber Security Society 2024-04

Research Title

Creating business value from cyber resilience.

Moving towards antifragility through organizational learning.



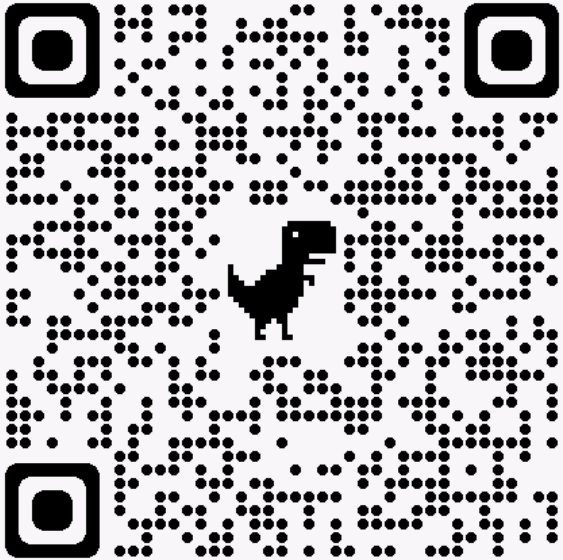
Index.md

1. Who am I

2. Business relevance
3. Academic relevance
4. The research
   a. Questions
   b. Design
   c. Planning

5. Q&A

6. ~~Core Concepts~~
   ~~Mental Models~~
   ~~Theory Building~~
7. ~~Literature Review WIP~~




Who am I

Organisational Resilience
Antifragility Architect
Trusted Advisor

@Edzob
(.com, LinkedIn, Twitter)

Apply

Share

Research

Consultancy for
7 Sectors,
40+ Clients,
50+ Assignments
from infra
to business strategy

Open Universiteit www.ou.nl
Antwerp Management School
HOGESCHOOL UTRECHT

Conferences & incompany training

Multiple whitepapers
Thesis/IEEE ~6.000 reads
40+ Blogs
Quoted in Books and Theses

1992 - 2006	*your* IT guy
2006 - 2020	Sogeti
2021 - 2023	Xebia
2024 - tbd	

PhD Student Cyber Resilience	2021-11 - tbd
MSc Enterprise Architecture	2018 - 2020
BSc Business Information Systems	2004 - 2006
ASc Computer Science	1999 - 2003

university of groningen
Hanzehogeschool Groningen
University of Applied Sciences
Antwerp Management School
Open Universiteit

Organisational Resilience
Antifragility Architect
Trusted Advisor

@Edzob
(.com, LinkedIn, Twitter)

Internships 2005-2006

BAARSMA WINES

heart for vital ict

Consultant @ Sogeti 2006 - 2020

Ministerie van Financiën

Ziggo

VISMA | raet

AIRFRANCE KLM Martinair CARGO

kpn

VfPf

achmea

KAS BANK

LINDORFF

Rijksdienst voor Ondernemend Nederland

AIRFRANCE KLM

IGNATION

sogeti Part of Capgemini

NYENRODE BUSINESS UNIVERSITEIT

ProRail

HAN UNIVERSITY OF APPLIED SCIENCES

mborijnland

Raad voor Rechtsbijstand

Consultant @ Xebia 2021 - 2023

Witteveen+Bos

Syntess Software

nationale nederlanden

sdworx

ASML

Xebia

anwb

SURF

topicus

LELY

NYENRODE BUSINESS UNIVERSITEIT

The business relevance
Why does it matter

The business relevance

Business impact security incidents

Nieuws

Minister: tekort aan cyberspecialisten op arbeidsmarkt algemeen probleem

dinsdag 16 april 2024, 16:17 door **Redactie**, 27 **reacties**

Demissionair minister Adriaansens van Economische Zaken komt binnenkort met een rapport over het tekort aan cybersecurityspecialisten op de arbeidsmarkt. Dat liet de minister vorige week weten tijdens een overleg van de vaste commissie voor Digitale Zaken over **online veiligheid en cybersecurity**.

Cyber blackmailers have stolen and published what is probably the most comprehensive data set on Swiss citizens abroad. How was this possible?

July 4, 2023 - 09:00 — 7 minutes

Balz Rigendinger

Other languages: 6

In mid-May, a stolen data set appeared on the darknet. The content was information about subscribers to *Swiss Review*. This is a federal government magazine that keeps Swiss citizens abroad up to date on developments in their home country.

The Register

Microsoft worker accidentally exposes 38TB of sensitive data in GitHub blunder

Included secrets, private keys, passwords, 30,000+ internal Teams messages

Jessica Lyons Hardcastle — Mon 18 Sep 2023 // 18:03 UTC

Deutsche Bank, ING, and Postbank impacted by MOVEit hack

Updated on: 13 July 2023

Stefanie Schappert, Senior journalist

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom

WSJ wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

May 19, 2021

The Register

Software

Microsoft's Azure mishap betrays an industry blind to a big problem

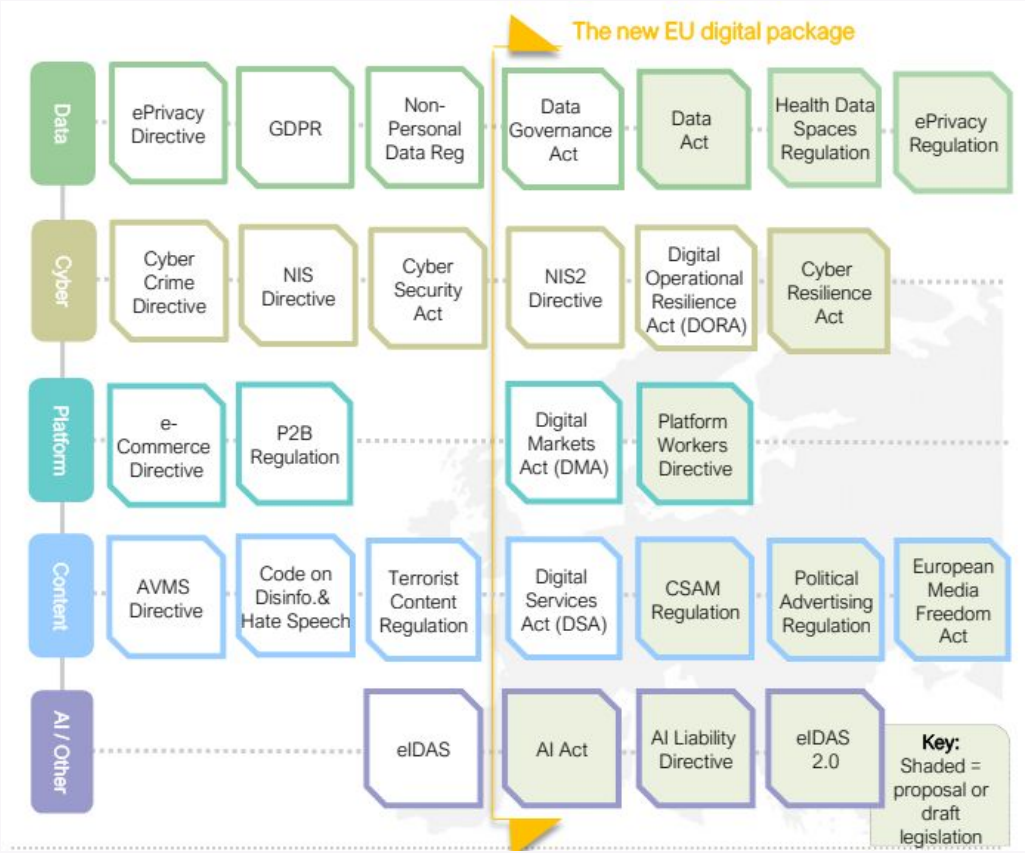
If a tiny typo brings down half of Brazil, perhaps we're the nuts

Rupert Goodwins
Mon 12 Jun 2023 // 08:30 UTC

- https://en.wikipedia.org/wiki/Swiss_Leaks
- https://cybernews.com/security/deutsche-ing-postbank-impacted-moveit-hack-clop/
- https://www.theregister.com/2023/09/18/more_microsoft_token_trouble
- https://www-theregister-com.cdn.ampproject.org/c/s/www.theregister.com/AMP/2023/06/12/comment
- https://www.swissinfo.ch/eng/politics/data-leak-affects-425-000-swiss-abroad/48628744
- https://www.security.nl/posting/838054/Minister%3A+tekort+aan+cyberspecialisten+op+arbeidsmarkt+algemeen+probleem

The business relevance

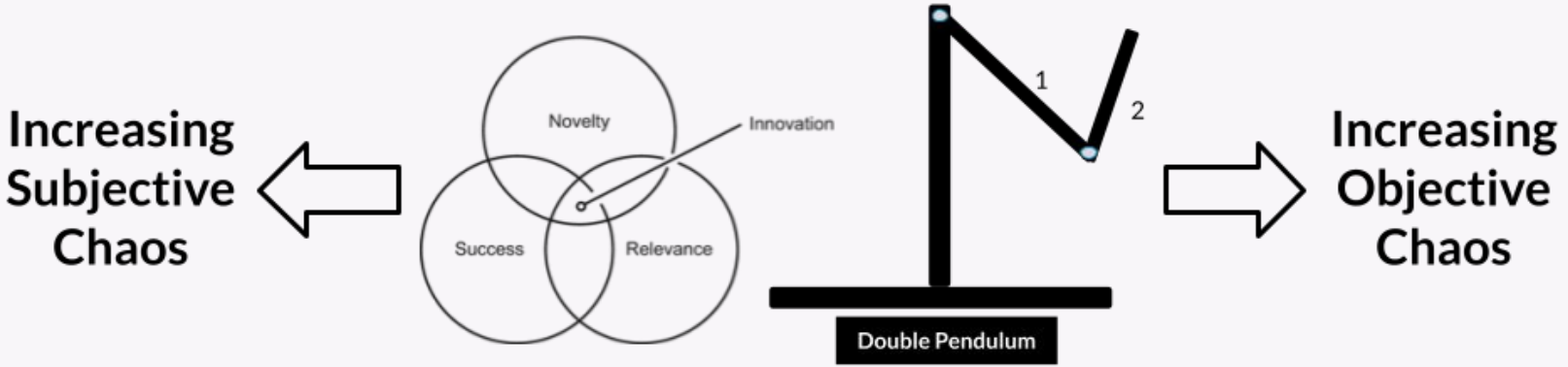
Increased EU (GDPR, NIS2, CRA, DORA, RED, …) and US law



- At a glance: A guide to the EU's new digital package January 2023 Guillaume Couneson https://www.linklaters.com/en/insights/blogs/digilinks/2022/november/eu---dga-data-act-nisd2-dsa---confused

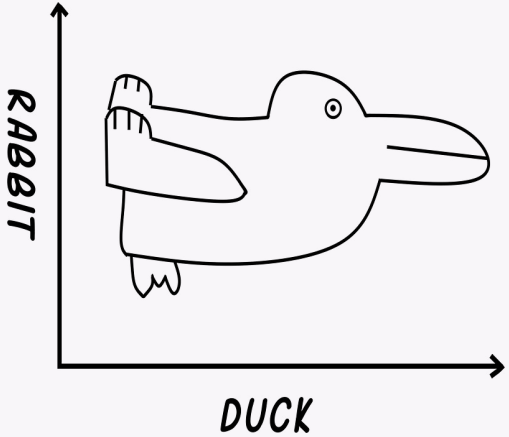
The business relevance

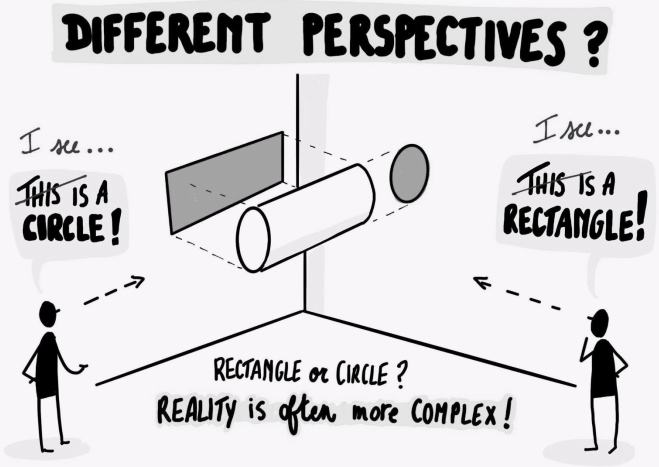
The challenge is fundamental



- Huber, D., Kaufmann, H., and Steinmann, M. (2017). Innovation: An Abiding Enigma, pages 11–19. Springer International Publishing, Cham. https://books.google.nl/books?id=rzckDwAAQBAJ
- Shinbrot, T., Grebogi, C., Wisdom, J., & Yorke, J. A. (1992). Chaos in a double pendulum. American Journal of Physics, 60(6), 491–499. doi: 10.1119/1.16860.
- Derbyshire, J., & Wright, G. (2014). Preparing for the future: Development of an 'antifragile' methodology that complements scenario planning by omitting causation. Technological Forecasting and Social Change, 82, 215–225. doi: 10.1016/J.TECHFORE.2013.07.001.

Examples of Subjective Chaos - Perspective

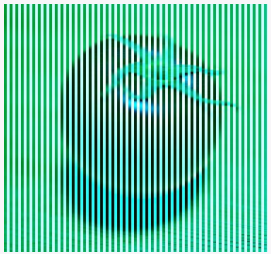




- https://scitechconnect.elsevier.com/lessons-from-the-dress-the-fundamental-ambiguity-of-visual-perception
- https://www.linkedin.com/posts/rafaelgiraldotenorio_entarch-activity-6681201385402376192-4MNK
- https://twitter.com/NicoleBeckwith/status/1277236284470280195/photo/1

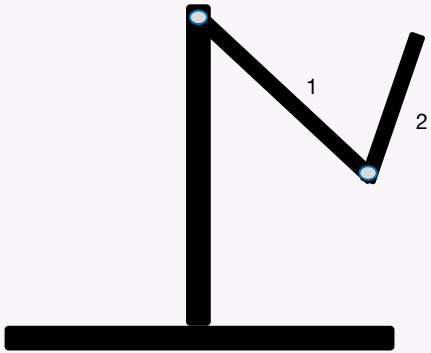
Examples of Subjective Chaos - Observation



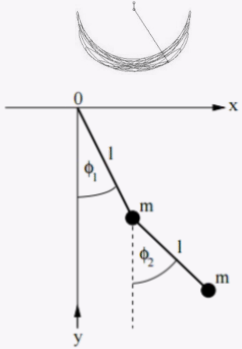



- Akiyoshi KITAOKA, Professor, Psychology, Ritsumeikan University, Osaka, Japan https://www.ritsumei.ac.jp/~akitaoka/index-e.html
- https://x.com/AkiyoshiKitaoka/status/1783764771130785985
- https://x.com/AkiyoshiKitaoka/status/1783765416286040153
- https://twitter.com/jimhejl/status/1452814882701824001
- https://twitter.com/AkiyoshiKitaoka/status/1568102162064113669
- https://writing.exchange/@XanIndigo/109966588561594572
- https://x.com/AkiyoshiKitaoka/status/1783767972924080326

Origins of Objective Chaos



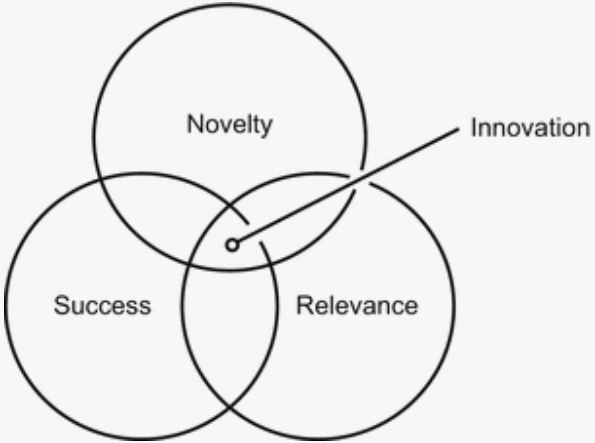
Double Pendulum



$$\frac{\mathrm{d}x}{\mathrm{d}t} = \sigma(y - x),$$

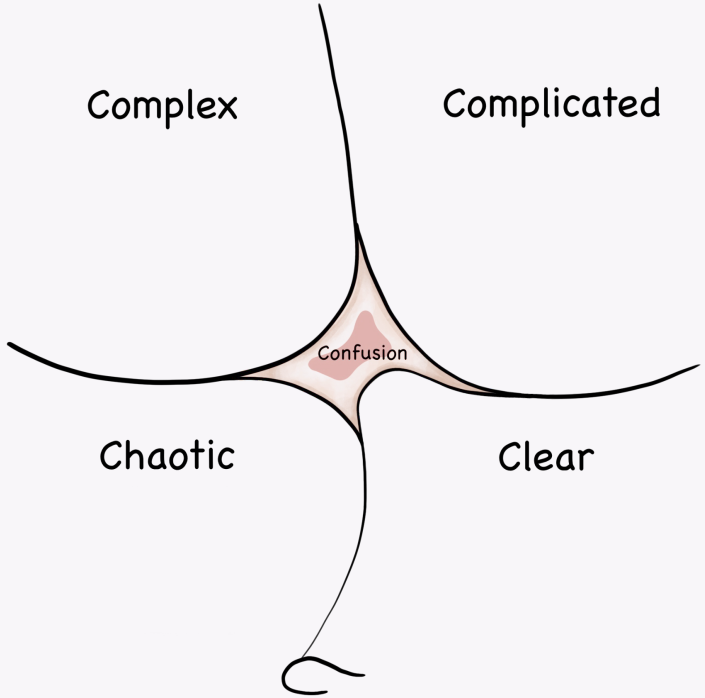
$$\frac{\mathrm{d}y}{\mathrm{d}t} = x(\rho - z) - y,$$

$$\frac{\mathrm{d}z}{\mathrm{d}t} = xy - \beta z.$$



- Huber, D., Kaufmann, H., and Steinmann, M. (2017). Innovation: An Abiding Enigma, pages 11–19. Springer International Publishing, Cham. https://books.google.nl/books?id=rzckDwAAQBAJ
- Shinbrot, T., Grebogi, C., Wisdom, J., & Yorke, J. A. (1992). Chaos in a double pendulum. American Journal of Physics, 60(6), 491–499. doi: 10.1119/1.16860.
- Lorenz, E. N. (1963). Deterministic nonperiodic flow. Journal of the atmospheric sciences, 20(2), 130–141. Doi: 10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2.

Sensemaking

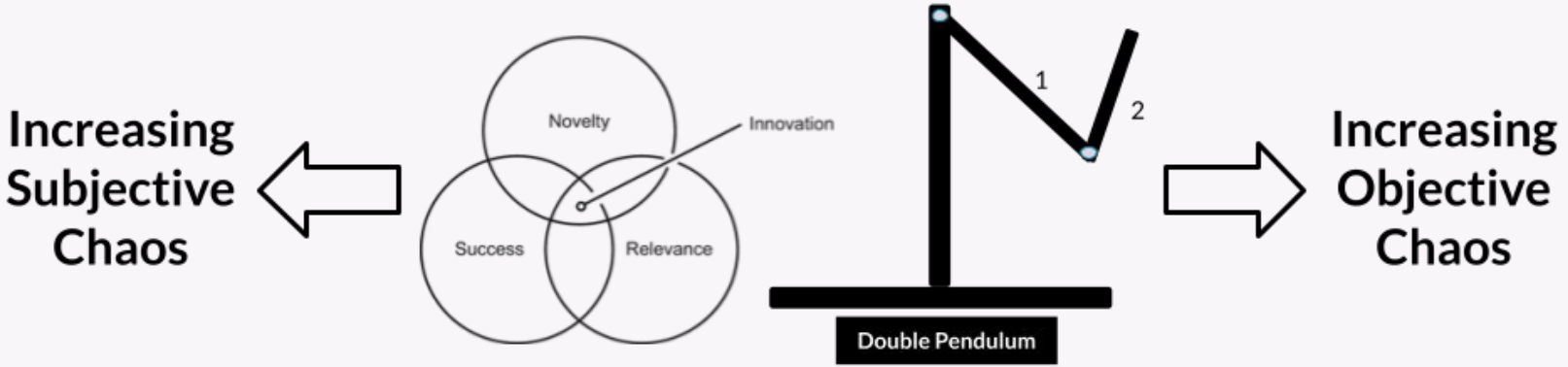


Hidden slide

- https://en.wikipedia.org/wiki/Cynefin_framework
- Snowden, David J.; Boone, Mary E. (2007). "A Leader's Framework for Decision Making". Harvard Business Review. 85 (11): 68–76. PMID 18159787.

The business relevance

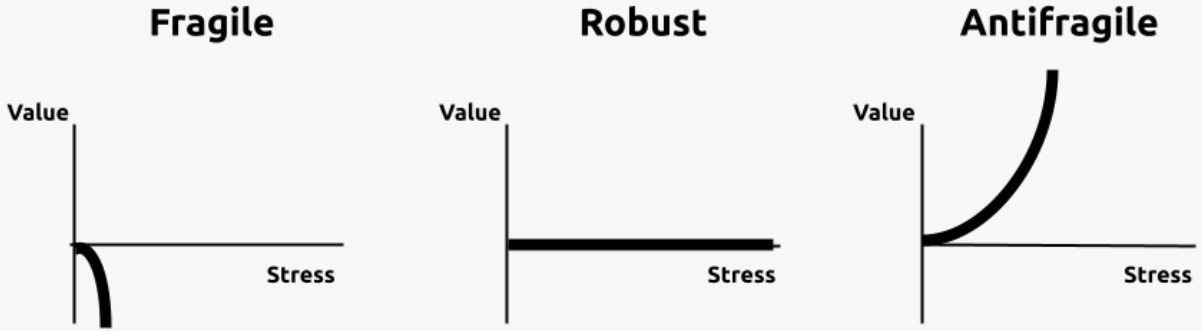
How to deal with the fundamental challenge?



- Huber, D., Kaufmann, H., and Steinmann, M. (2017). Innovation: An Abiding Enigma, pages 11–19. Springer International Publishing, Cham. https://books.google.nl/books?id=rzckDwAAQBAJ
- Shinbrot, T., Grebogi, C., Wisdom, J., & Yorke, J. A. (1992). Chaos in a double pendulum. American Journal of Physics, 60(6), 491–499. doi: 10.1119/1.16860.
- Derbyshire, J., & Wright, G. (2014). Preparing for the future: Development of an 'antifragile' methodology that complements scenario planning by omitting causation. Technological Forecasting and Social Change, 82, 215–225. doi: 10.1016/J.TECHFORE.2013.07.001.

The business objective

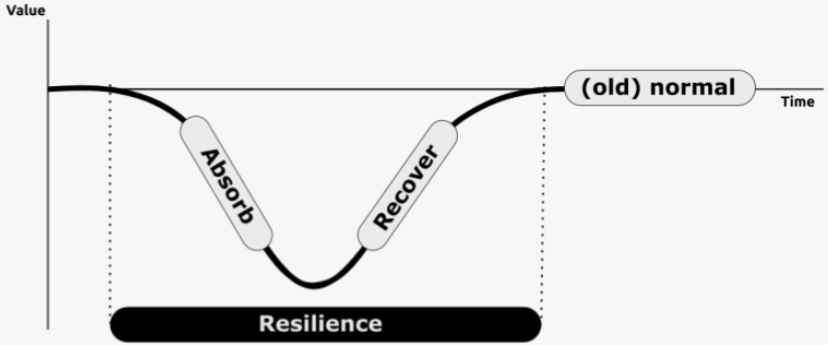
Is fragility an option? Antifragile is only counter to chaos.

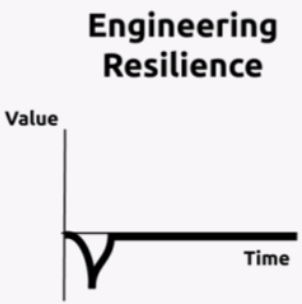


- Taleb, N. N. (2012). Antifragile: Things that gain from disorder (Vol. 3). Random House Trade Paperbacks.
- Botjes, E. A., van den Berg, M., van Gils, B., & Mulder, H. (2021). Attributes relevant to antifragile organizations. In J. P. A. Almeida, D. Bork, G. Guizzardi, M. Montali, H. A. Proper & T. P. Sales (Eds.), 2021 IEEE 23nd conference on business informatics (CBI) (pp. 62–71, Vol. 01). IEEE. doi: 10.1109/CBI52690.2021.00017

The business dilemma

‘Normal’ resilience is not enough, and it is the default language.

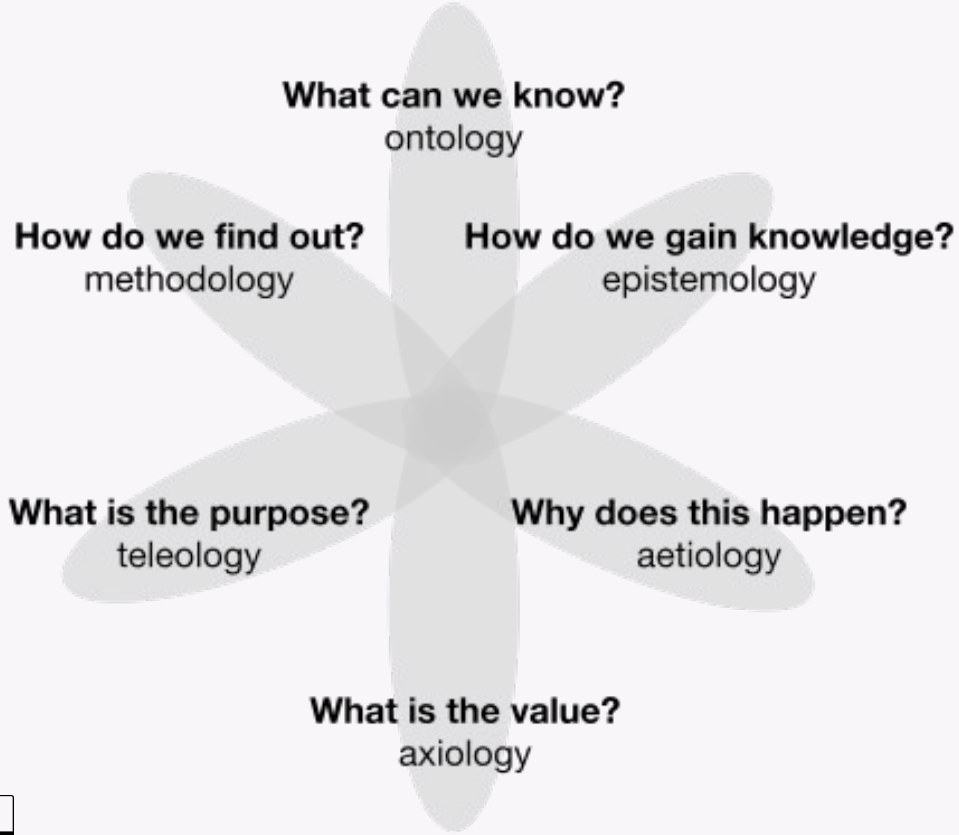




- Botjes, E. A., van den Berg, M., van Gils, B., & Mulder, H. (2021). Attributes relevant to antifragile organizations. In J. P. A. Almeida, D. Bork, G. Guizzardi, M. Montali, H. A. Proper & T. P. Sales (Eds.), 2021 IEEE 23nd conference on business informatics (CBI) (pp. 62–71, Vol. 01). IEEE. doi: 10.1109/CBI52690.2021.00017
- Martin-Breen, P. and Anderies, J. M. (2011). The bellagio initiative, background paper, resilience: A literature review. In Resilience: A Literature Review, Brighton:IDS. http://opendocs.ids.ac.uk/opendocs/handle/123456789/3692.
- Taleb, N. N. (2012). Antifragile: Things that gain from disorder (Vol. 3). Random House Trade Paperbacks.

The academic relevance
What don’t we know already

Research Lenses

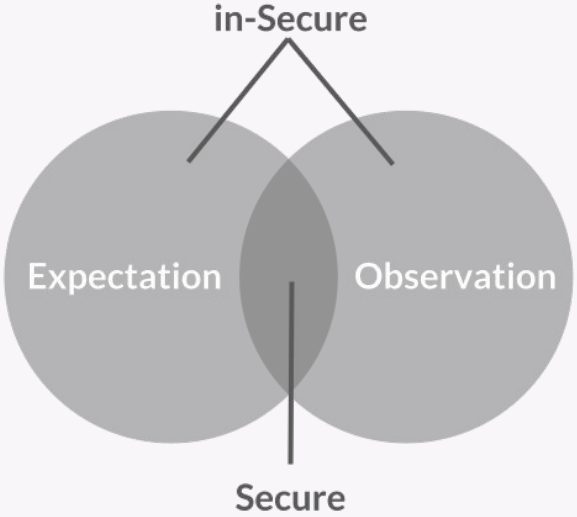


The academic relevance

What is Security?

What is Cyber Security?

What is Cyber Resilience?



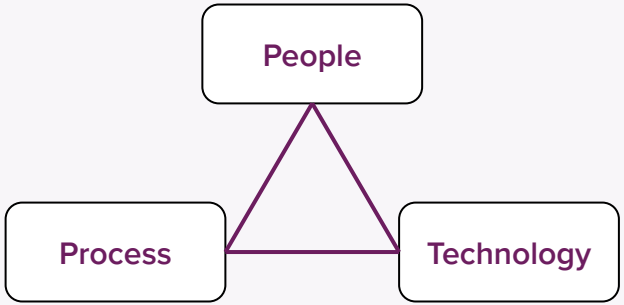
- Schneier, B. (2008). The psychology of security. International conference on cryptology in Africa, 5023, 50–79. Doi: 10.1007/978-3-540-68164-9_5.
- Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security. Behaviour & Information Technology, 29(3), 221–232. doi: 10.1080/01449290701679361.

The academic relevance

What is Security?

What is Cyber Security?

What is Cyber Resilience?



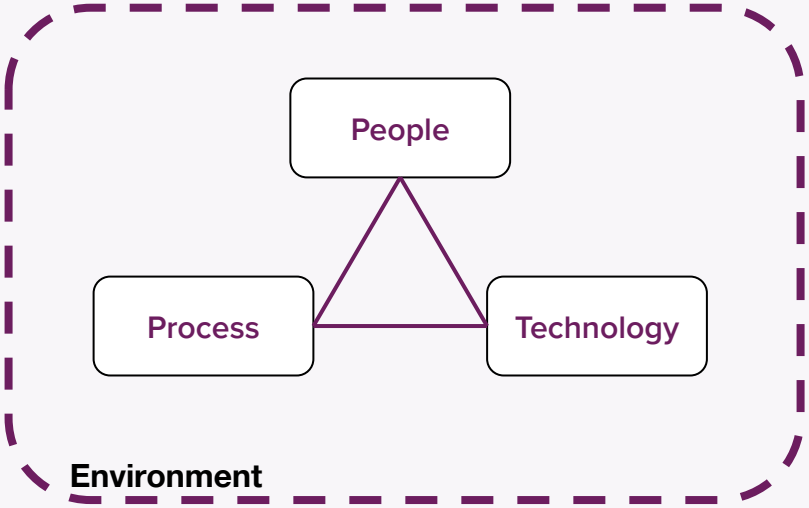
- Schneier, B. (2008). The psychology of security. International conference on cryptology in Africa, 5023, 50–79. Doi: 10.1007/978-3-540-68164-9_5.
- Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security. Behaviour & Information Technology, 29(3), 221–232. doi: 10.1080/01449290701679361.

The academic relevance

What is Security?

What is Cyber Security?

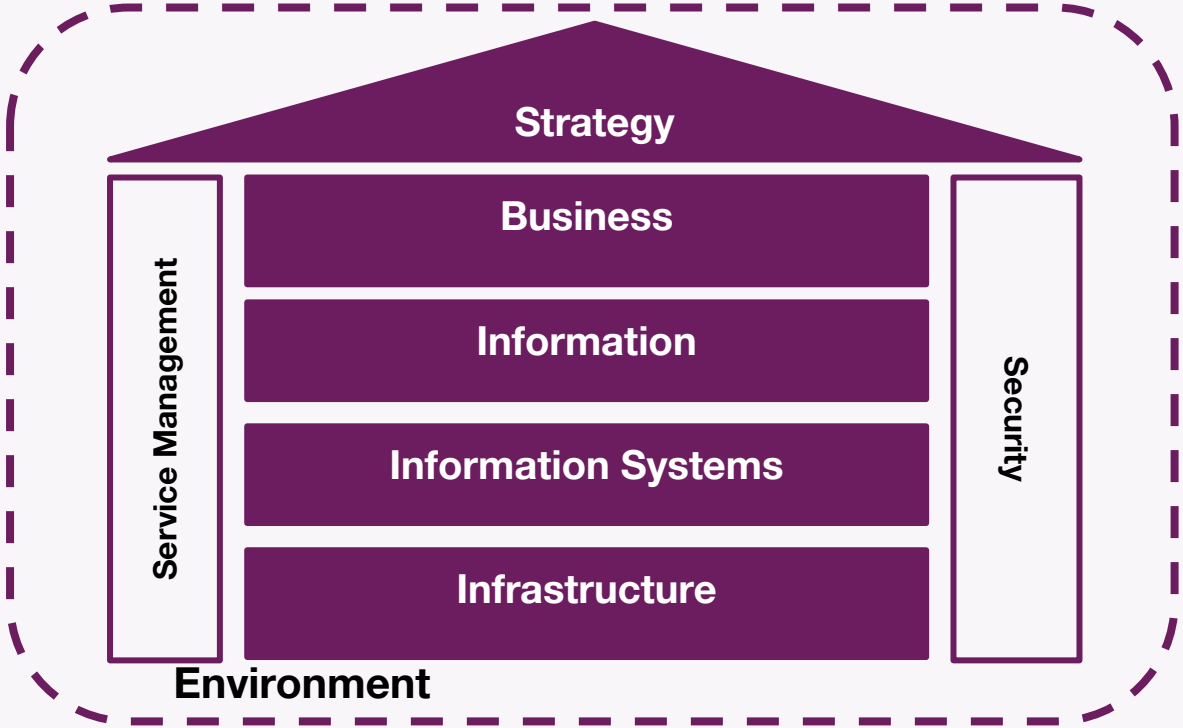
What is Cyber Resilience?



- Eling, Martin, Michael McShane, and Trung Nguyen. 2021. “Cyber Risk Management: History and Future Research Directions.” Risk Management and Insurance Review 24(1): 93–125. doi:10.1111/rmir.12169.

Cyber Resilience scope

Hidden slide



The academic relevance

What is Value?

What do we want to prevent, protect?

Do we want to exploit opportunities?

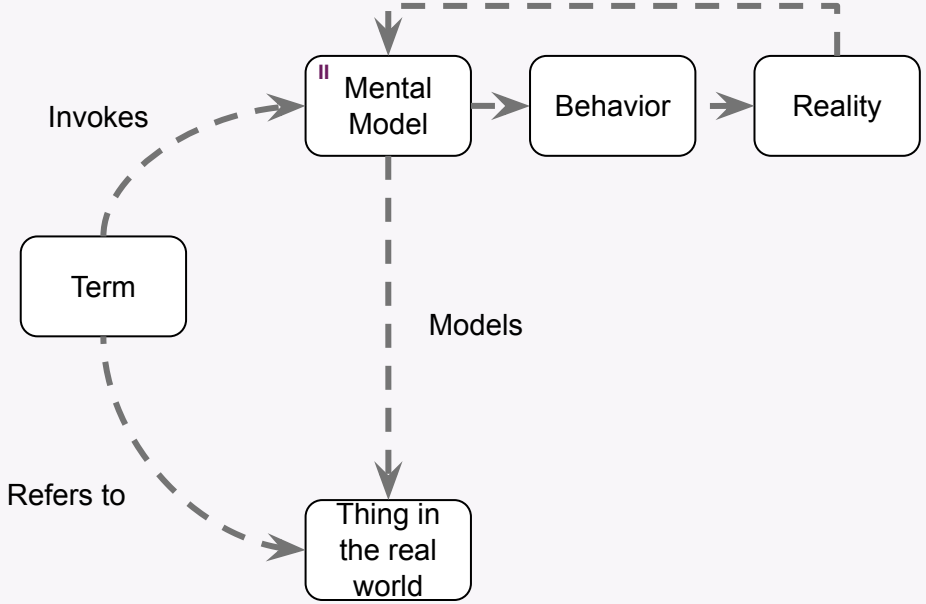
- Van Gils, B. (2023). Data in context: Models as enablers for managing and using data. Springer Nature Switzerland. doi: 10.1007/978-3-031-35539-4 https://link.springer.com/book/10.1007/978-3-031-35539-4
- Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security. Behaviour & Information Technology, 29(3), 221–232. doi: 10.1080/01449290701679361.
- Eling, Martin, Michael McShane, and Trung Nguyen. 2021. “Cyber Risk Management: History and Future Research Directions.” Risk Management and Insurance Review 24(1): 93–125. doi:10.1111/rmir.12169.

The academic relevance

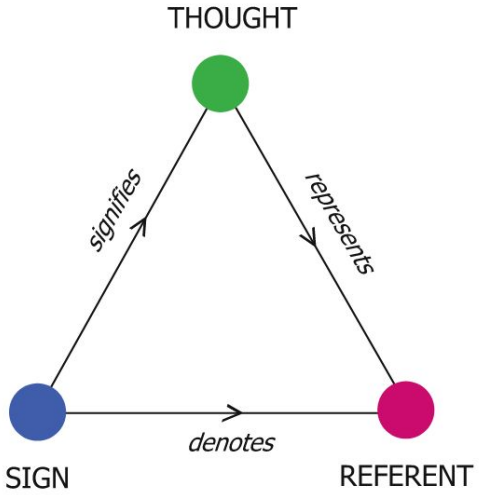
What is Value?

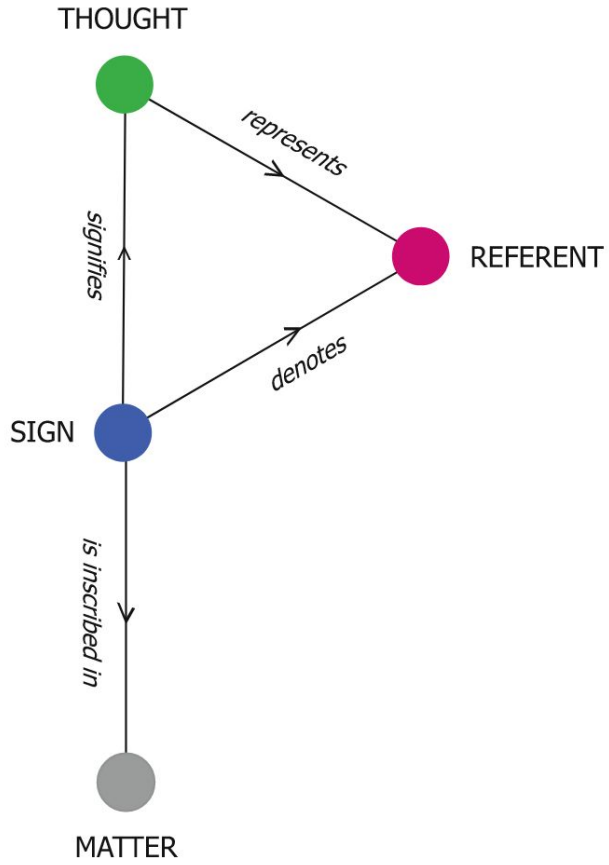
What do we want to prevent, protect?

Do we want to exploit opportunities?



- Hestenes, D. (2010). Modeling theory for math and science education. In Modeling students' mathematical modeling competencies, pages 13–41. Springer.
- Dietz, Jan L. G, and Hans B. F Mulder. 2020. Enterprise Ontology: A Human-Centric Approach to Understanding the Essence of Organisation. 1st ed. Cham, Switzerland: Springer International Publishing. doi:10.1007/978-3-030-38854-6. Fig 6.1 [Ogden and Richard's semiotic triangle]
- Ogden, C. K., et al. (1923). The meaning of meaning: A study of the influence of language upon thought and of the science of symbolism. International library of psychology, philosophy, and scientific method. , London: K. Paul, Trench, Trubner/Harcourt, Brace, xxxi, 1, 544p.





Hidden slide

Fig. 5.1 The adapted (left) and extended (right) semiotic triangle

- Dietz, Jan L. G, and Hans B. F Mulder. 2020. Enterprise Ontology: A Human-Centric Approach to Understanding the Essence of Organisation. 1st ed. Cham, Switzerland: Springer International Publishing. doi:10.1007/978-3-030-38854-6. Fig 6.1 [Ogden and Richard's semiotic triangle]

Hidden slide

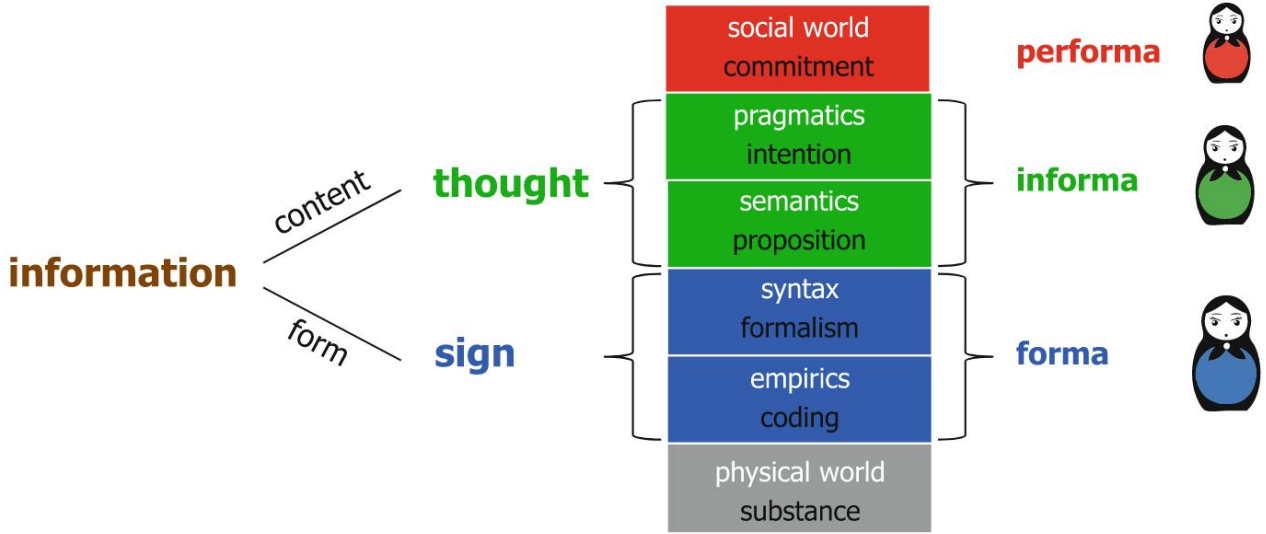


Fig. 5.2 The semiotic ladder

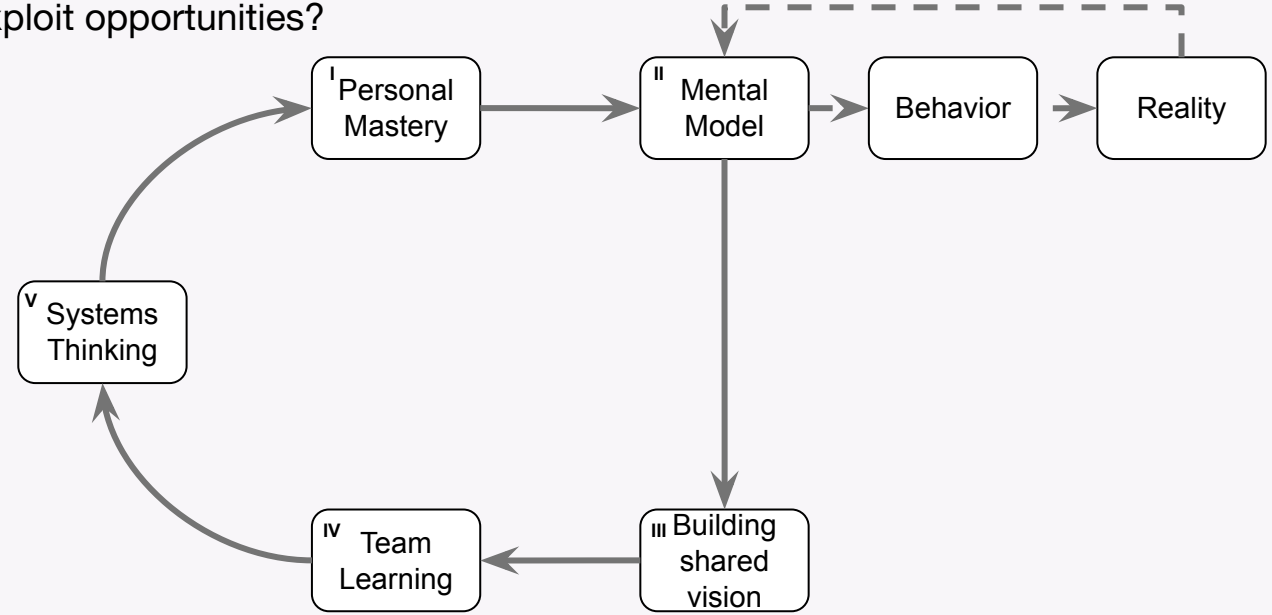
- Dietz, Jan L. G, and Hans B. F Mulder. 2020. Enterprise Ontology: A Human-Centric Approach to Understanding the Essence of Organisation. 1st ed. Cham, Switzerland: Springer International Publishing. doi:10.1007/978-3-030-38854-6. Fig 6.1 [Ogden and Richard's semiotic triangle]

The academic relevance

What is Value?

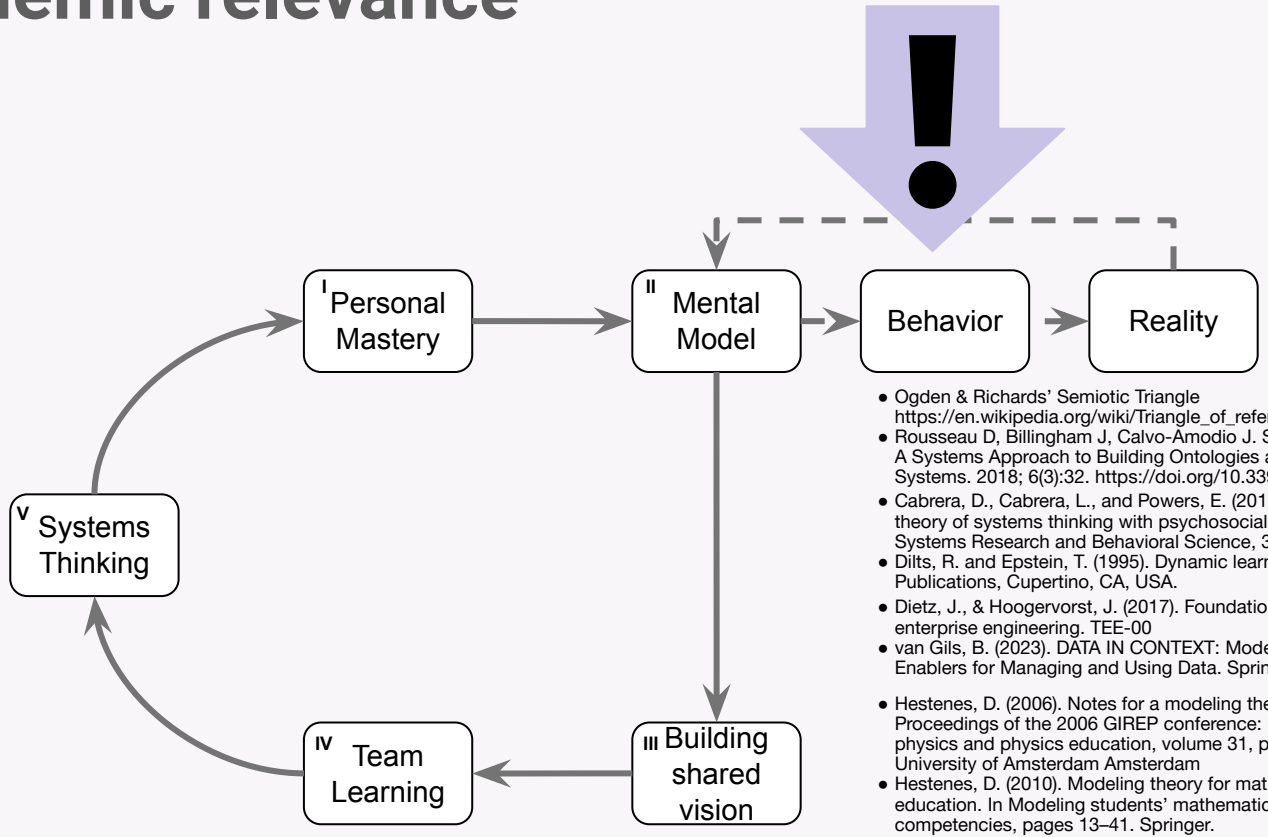
What do we want to prevent, protect?

Do we want to exploit opportunities?



- Senge, P. M. (1990). The Fifth Discipline: The Art and Practice of the Learning organisation. A Currency book. Doubleday/Currency, New York, NY, USA.
- Hestenes, D. (2010). Modeling theory for math and science education. In Modeling students' mathematical modeling competencies, pages 13–41. Springer.

The academic relevance



- Ogden & Richards' Semiotic Triangle https://en.wikipedia.org/wiki/Triangle_of_reference
- Rousseau D, Billingham J, Calvo-Amodio J. Systemic Semantics: A Systems Approach to Building Ontologies and Concept Maps. Systems. 2018; 6(3):32. https://doi.org/10.3390/systems6030032
- Cabrera, D., Cabrera, L., and Powers, E. (2015). A unifying theory of systems thinking with psychosocial applications. Systems Research and Behavioral Science, 32(5):534–545.
- Dilts, R. and Epstein, T. (1995). Dynamic learning. Meta Publications, Cupertino, CA, USA.
- Dietz, J., & Hoogervorst, J. (2017). Foundations of enterprise engineering. TEE-00
- van Gils, B. (2023). DATA IN CONTEXT: Models as Enablers for Managing and Using Data. Springer.
- Hestenes, D. (2006). Notes for a modeling theory. In Proceedings of the 2006 GIREP conference: Modeling in physics and physics education, volume 31, page 27. University of Amsterdam Amsterdam
- Hestenes, D. (2010). Modeling theory for math and science education. In Modeling students' mathematical modeling competencies, pages 13–41. Springer.
- Senge, P. M. (1990). The Fifth Discipline: The Art and Practice of the Learning organisation. A Currency book. Doubleday/Currency, New York, NY, USA

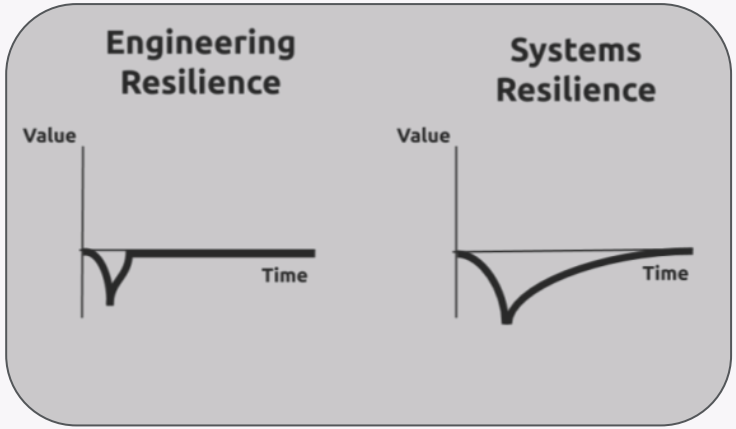
The academic relevance

What is Value?

What do we want to prevent, protect?

Do we want to exploit opportunities?

Most (business) literature is focused on prevent and minimize, less on exploitation



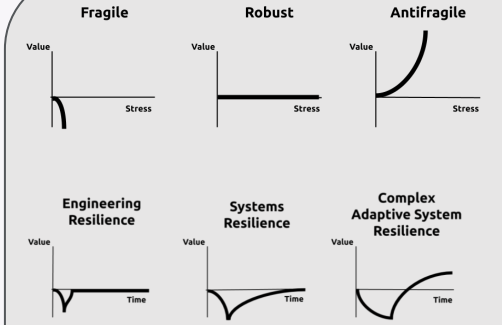
- Botjes, E. A., van den Berg, M., van Gils, B., & Mulder, H. (2021). Attributes relevant to antifragile organizations. In J. P. A. Almeida, D. Bork, G. Guizzardi, M. Montali, H. A. Proper & T. P. Sales (Eds.), 2021 IEEE 23nd conference on business informatics (CBI) (pp. 62–71, Vol. 01). IEEE. doi: 10.1109/CBI52690.2021.00017

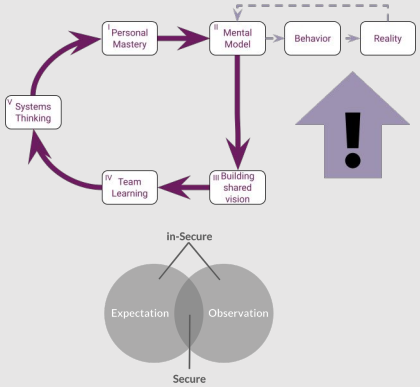
The academic relevance

What is Value?

What do we want to prevent, protect?

<u>How</u> we want to exploit opportunities?





Cyber Resilience Maturity Model

The research
Peeling the onion

Research Questions

How do existing CRMMs and Antifragility relate
RQ1: Is there a Cyber Resilience Maturity Model (CRMM) that adequately addresses the exploitation of unforeseen events, as defined in the ISO 31000 on risk management?

Applying CRMM and investigate resilience enhancement
RQ2: Does the (extended) Cyber Resilience Maturity Model (CRMM) offer guidance and value when applied by organizations?

Retroduction and replication
RQ3: What are the key lessons learned from the application of the Cyber Resilience Maturity Model (CRMM) and how can these lessons be incorporated in to refined version of the CRMM?

- https://www.overleaf.com/read/wncjywdqdhpc#94f53a

Research Questions

How do existing CRMMs and Antifragility relate
RQ1: Is there a Cyber Resilience Maturity Model (CRMM) that adequately addresses the exploitation of unforeseen events, as defined in the ISO 31000 on risk management?
RQ1.1: Identify existing CRMMs;
RQ1.2: Retrieve existing criteria for a sound MM and CRMMs;
RQ1.3: Develop criteria for Antifragility-supportive CRMMs;
RQ1.4: Evaluate existing CRMMs against Antifragility criteria;
RQ1.5: Evaluate existing CRMMs against the identified criteria for a sound MM and CRMM;
RQ1.6: Change an existing CRMM accordingly when needed.

- https://www.overleaf.com/read/wncjywdqdhpc#94f53a

Applying CRMM and investigate resilience enhancement
RQ2: Does the (extended) Cyber Resilience Maturity Model (CRMM) offer guidance and value when applied by organizations?
RQ2.1: Assess resilience improvement;
RQ2.2: Investigate perceived value from unforeseen event exploitation;
RQ2.3: Verify reproducibility in different contexts;
RQ2.4: Evaluate long-term effects.)

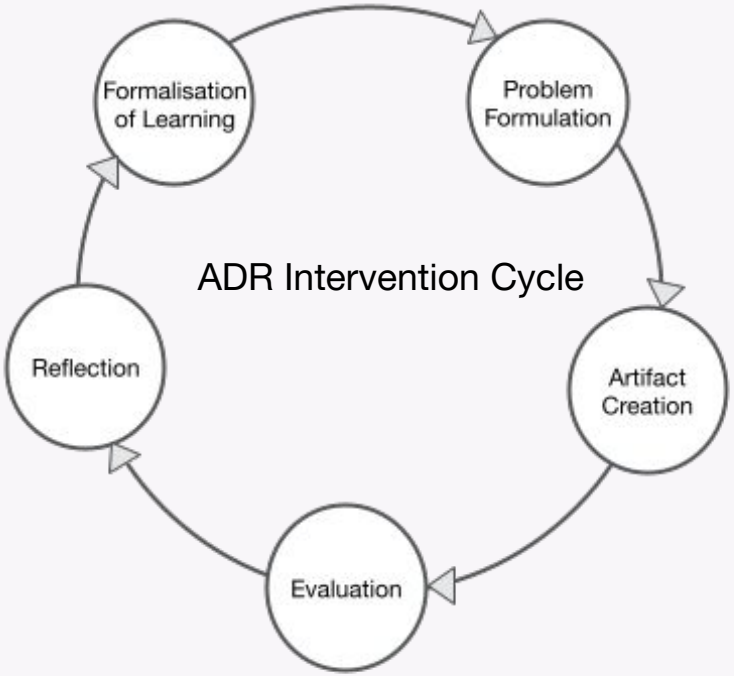
Retroduction and replication
RQ3: What are the key lessons learned from the application of the Cyber Resilience Maturity Model (CRMM) and how can these lessons be incorporated in to refined version of the CRMM?
RQ3.1: Lessons learned from the application of the CRMM;
RQ3.2: Retroduction on identified structures;
RQ3.3: Incorporated lessons learned into a refined CRMM;
RQ3.4: Replicability of CRMM application with refined CRMM)

Research Design

Action Design Research seems a logical choice for research methodology.

Cyber resilience, is about
risk management of the organisation (holistic)
combined with
cyber security (holistic) and both are adaptive.

A Maturity Model is used to asses, plan, execute and re-asses.

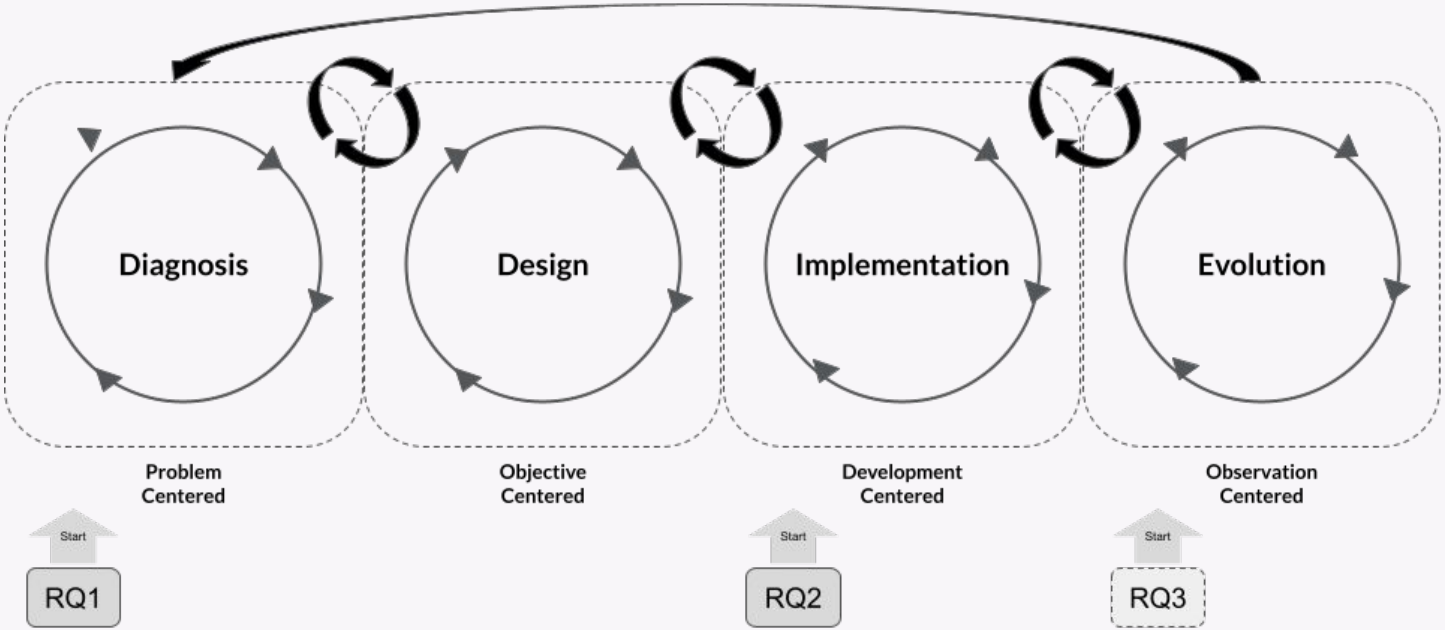


- Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. MIS Quarterly, 35(1), 37–56. doi: 10.2307/23043488.
- Susman, G. I., & Evered, R. D. (1978). An assessment of the scientific merits of action research. Administrative Science Quarterly, 23(4), 582–603. doi: 10.2307/2392581.
- Mullarkey, M. T., & Hevner, A. R. (2019). An elaborated action design research process model (P. Ågerfalk, Ed.). European Journal of Information Systems, 28(1), 6–20. doi: 10.1080/0960085X.2018.1451811.

Research Design - eADR

Elaborated ADR (eADR) combines Action Design Research with Design Science Research.

eADR is designed to tackle wicked problems, in organisational context and supports iterative research.



- Mullarkey, M. T., & Hevner, A. R. (2019). An elaborated action design research process model (P. Ågerfalk, Ed.). European Journal of Information Systems, 28(1), 6–20. doi: 10.1080/0960085X.2018.1451811.

Research Roadmap

2021-11	start	—	
2022	1st & 2nd proposal	—	
2023	—	—	Leave employer
2024	3th proposal	Conf Article	
2024	RQ1.1 - RQ1.5	Conf Article	This article will provide an overview of the criteria selected to evaluate existing CRMMs, concluding with the match and mismatch with these criteria.
2024	RQ1.6	Conf Article	This article will address the selected CRMM that fits the criteria, or most likely describe the newly created CRMM.
2025	RQ2	Journal Article	This article will address the effectiveness and (un)proven causality of (new) CRMM in regard to guiding organizations with improving their antifragile behavior.
2026	RQ3	Journal Article	This article will address the observed effects of continued use of the CRMM on the users, their context and the CRMM itself.
2027	RQ1-3	Dissertation	

Research Roadmap

2018-2020	Start Msc	MSc Thesis	MSc EA @ AMS - summa cum laude
2021	IEEE Publication	Conf Paper	
2021-11	Start PhD	—	
2022	1st & 2nd proposal	—	
2023	XXXXX	XXXX	No PhD work - leave employer
2024	3th proposal	Conf Article	When research proposal is approved, then present it a a conference for publication
2024	RQ1.1 - RQ1.5	Conf Article	This article will provide an overview of the criteria selected to evaluate existing CRMMs, concluding with the match and mismatch with these criteria.
2024	RQ1.6	Conf Article	This article will address the selected CRMM that fits the criteria, or most likely describe the newly created CRMM.
2025	RQ2	Journal Article	This article will address the effectiveness and (un)proven causality of (new) CRMM in regard to guiding organizations with improving their antifragile behavior.
2026	RQ3	Journal Article	This article will address the observed effects of continued use of the CRMM on the users, their context and the CRMM itself.
2027	RQ1-3	Dissertation	

Research Infrastructure

Research Support System

Hidden slide

Promotion team (3 profs)

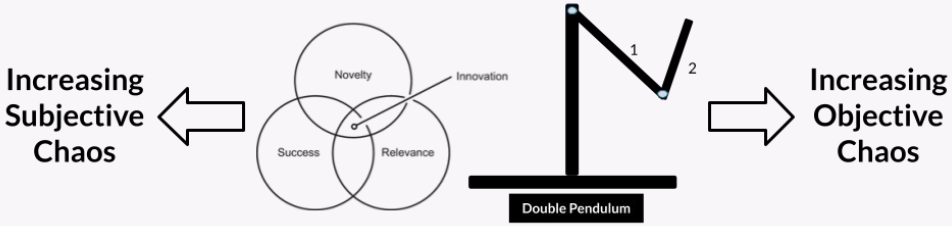
Senior Professors from AMS

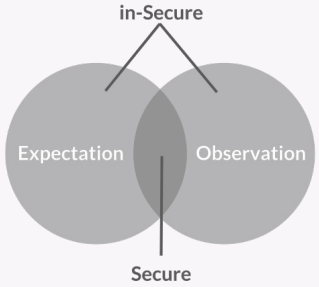
Weekly research group Mastermind style, including researchers from various universities and countries (NL, BE, CA)

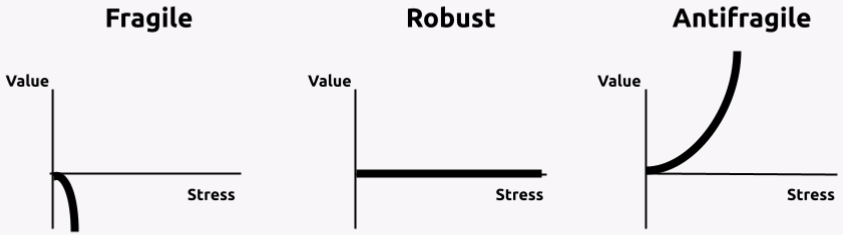
MSc students AMS

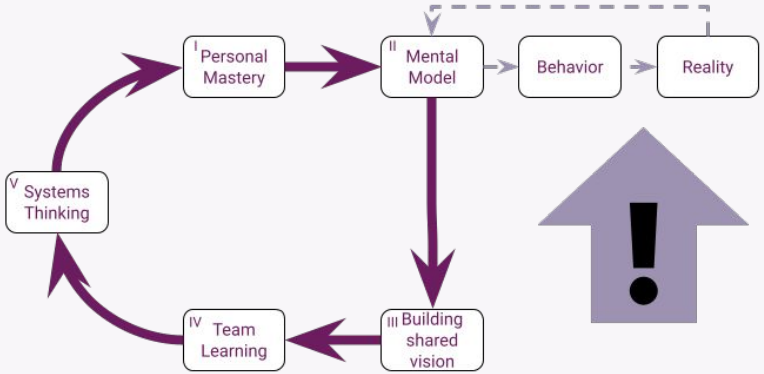
MSc students HU


The conceptual models
Lenses on reality









RQ1: Is there a Cyber Resilience Maturity Model (CRMM) that adequately addresses the exploitation of unforeseen events, as defined in the ISO 31000 on risk management?

RQ2: Does the (extended) Cyber Resilience Maturity Model (CRMM) offer guidance and value when applied by organizations?

RQ3: What are the key lessons learned from the application of the Cyber Resilience Maturity Model (CRMM) and how can these lessons be incorporated in to refined version of the CRMM?