Digital Business Transformation Forum | GDI Rüschlikon, Oct 2025

AI & Cyber Security

Beyond hypes and trends

Dr. Stefan Frei

Security Architect @ Rheinmetall Air Defence / Lecturer @ ETHZ

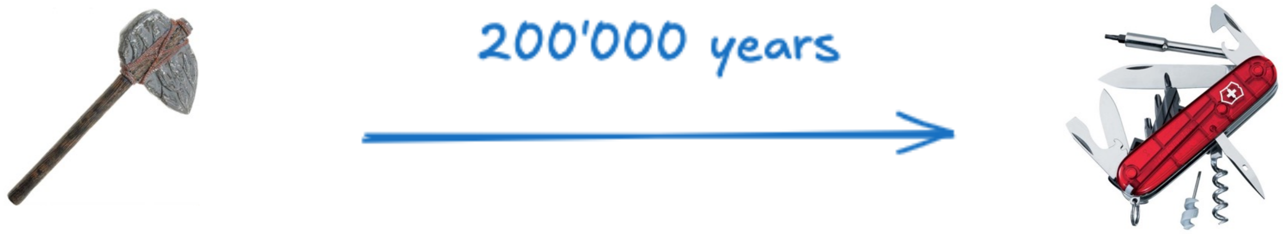
frei@techzoom.net | Web https://techzoom.net | BSky stefanfrei.bsky.social

What are the biggest challenges in cyber security?

&

The role of Artificial Intelligence

Decreasing time to learn



200'000 years

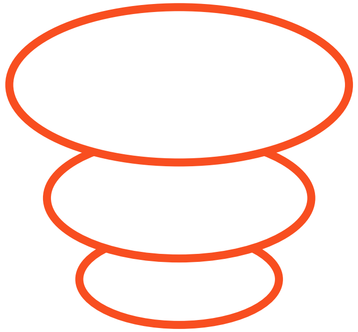
60 years

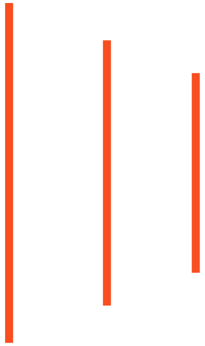
History shows: Attackers adapt faster than defenders

Cyber is abstract / invisible

TRADITIONAL

DIGITAL





SECURITY

ENGINEERING

BUSINESS

You can not manage what you can not measure

- Humans are new to technology and abstract risks
- Security risks are invisible without testing

no training needed to act

CONSEQUENCES

- Accumulation of silent risks
- Illusion of control

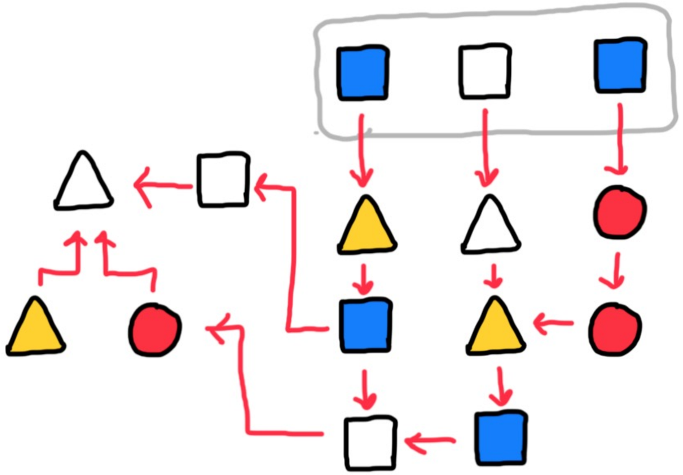
?

training & testing needed to act

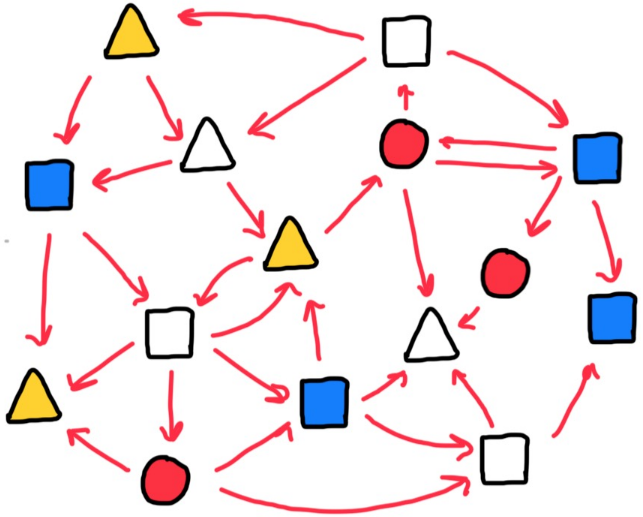
People need highly visible incidents before they act

Increasing Complexity

Different kinds of complexity



Simple



Complex

tightly coupled

software intensive

interconnected

Model confusion

A SIMPLE SYSTEM CAN BE SIMPLIFIED INTO SUBSYSTEMS

One can solve each simplified subsystem to solve the whole

A COMPLEX SYSTEM CANNOT BE SIMPLIFIED

Requires different methodologies for its investigation

- *Full knowledge of all components can not predict system behavior (emerging properties)*

Decreasing predictability

INCREASING COMPLEXITY

- Increasing interaction of humans, devices, apps, services, ..
- Novel types of interactions lead to novel attacks which cannot be detected

CONSEQUENCES

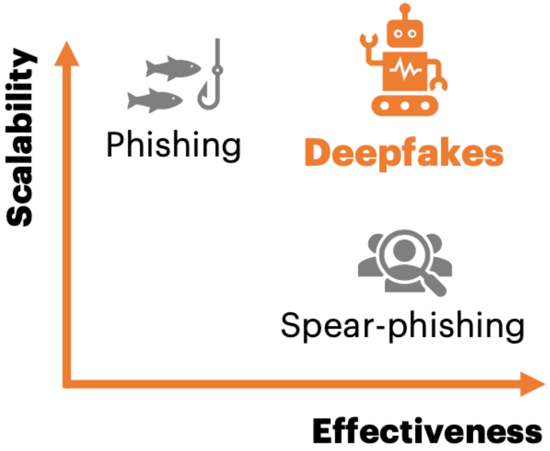
- Decreasing predictability
- 100% prevention is not possible

Artificial Intelligence

AI attack automation & scale

Attack Humans

deception / misinformation



Scalability

Phishing

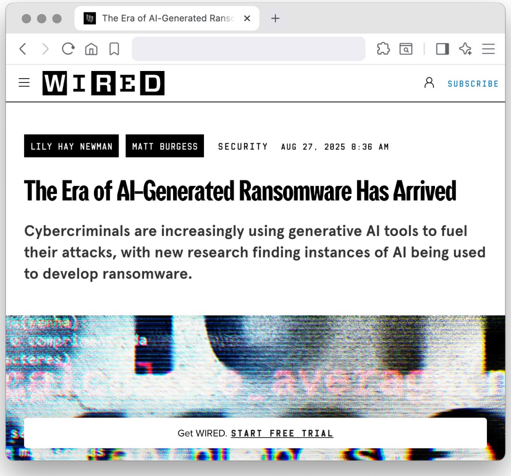
Deepfakes

Spear-phishing

Effectiveness

Attack Systems

automated attack generation



LILY HAY NEWMAN MATT BURGESS SECURITY AUG 27, 2025 8:36 AM

The Era of AI-Generated Ransomware Has Arrived

Cybercriminals are increasingly using generative AI tools to fuel their attacks, with new research finding instances of AI being used to develop ransomware.

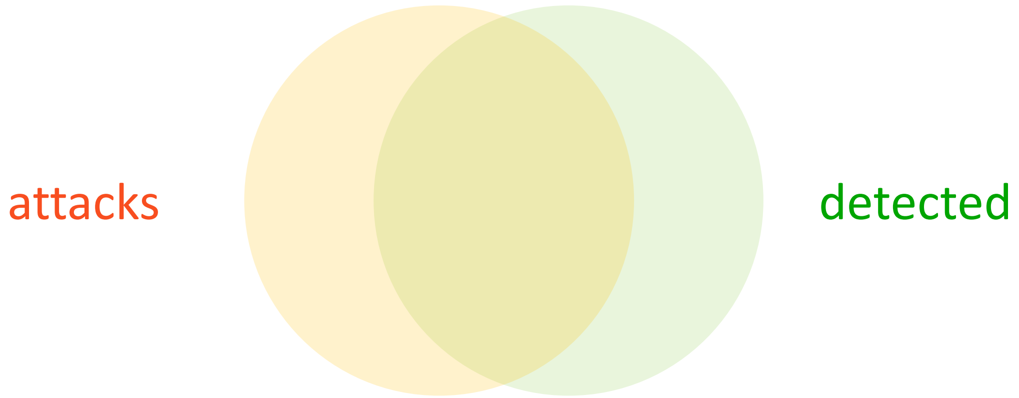
Get WIRED. START FREE TRIAL

INDUSTRY RESPONSE

We stop more threats with an additional layer of AI-powered detection ($$$)

The cost of detection errors

Any detector has to balance inevitable false alerts and missed detections



ATTACKER

- must be right only once
- cost of a detected attack is low

DEFENDER

- must be always right
- cost of a false alarm is high

interruptions, alert fatigue, ..

An asymmetry that systematically benefits attack over defense

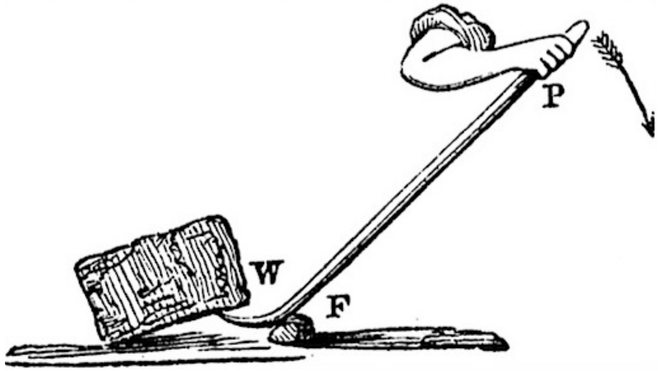
What can we do?

Control impact, not attack

- Control impact (which we know), not probability of event (we don’t know)
- Build systems that absorb disruptions and recover fast (resilience)

STRATEGIC APPROACH

- Protect critical assets rather than anticipating every possible attack
- This yields a smaller and manageable set of potential losses we need to address



The role of testing

Failures are inevitable if you try something new

No failure means you are optimizing not innovating

View failures as learning opportunities

“The cause of the failure was not even on our risk list”

- No tool or theory would have identified or prevented the failure!

Conclusion

Not seeing a tsunami, an economic event, or a cyber-attack coming is excusable.

Building something fragile to them is not.

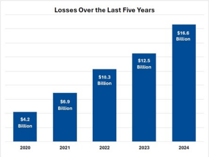
- Complexity is not the enemy of security
- Bad design is!

- Focus on aspects of the problem that we can control

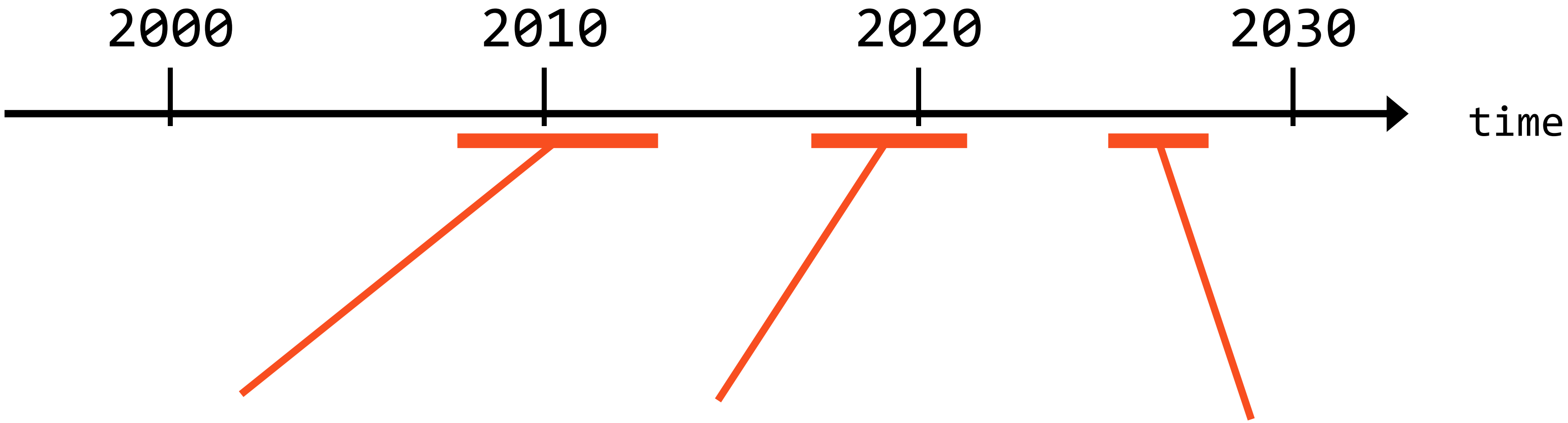
- Identify asymmetries between attack and defense to inform smart investment

Appendix

Cyber Security: Silver bullets & hypes



losses



Cloud

solves
cyber security

Blockchain

solves
cyber security

AI

solves
cyber security