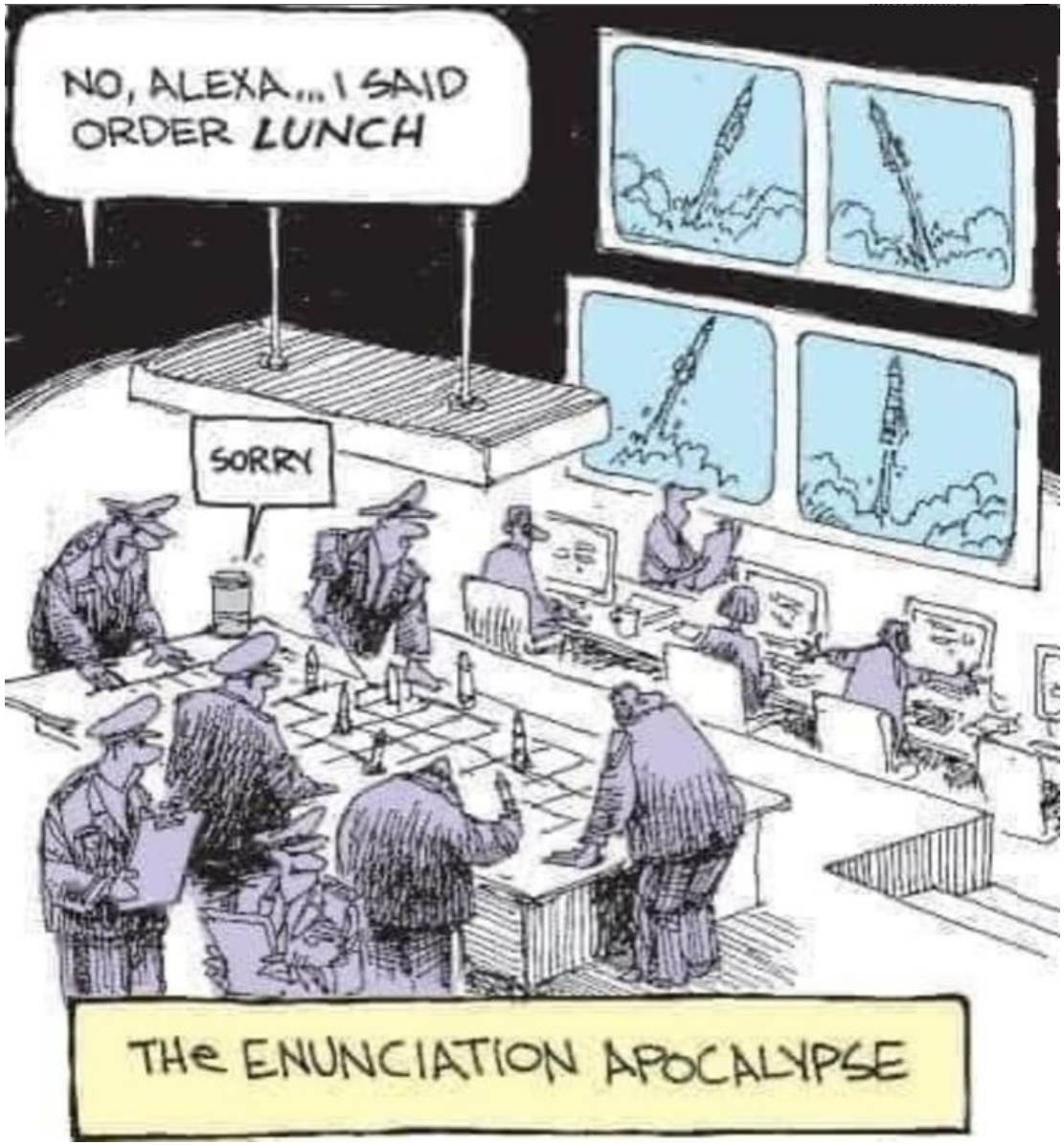
# Selected Security News

H. Lubich

lubich@acm.org


NO, ALEXA... I SAID ORDER LUNCH
SORRY
THE ENUNCIATION APOCALYPSE


CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE
Tallinn 2022
RESEARCH REPORT
Military Movement: Risks from 5G Networks
CCDCOE


FIGURE 10. THREATS RELATED TO 5G SUBSYSTEMS, ENISA THREAT LANDSCAPE FOR 5G NETWORKS

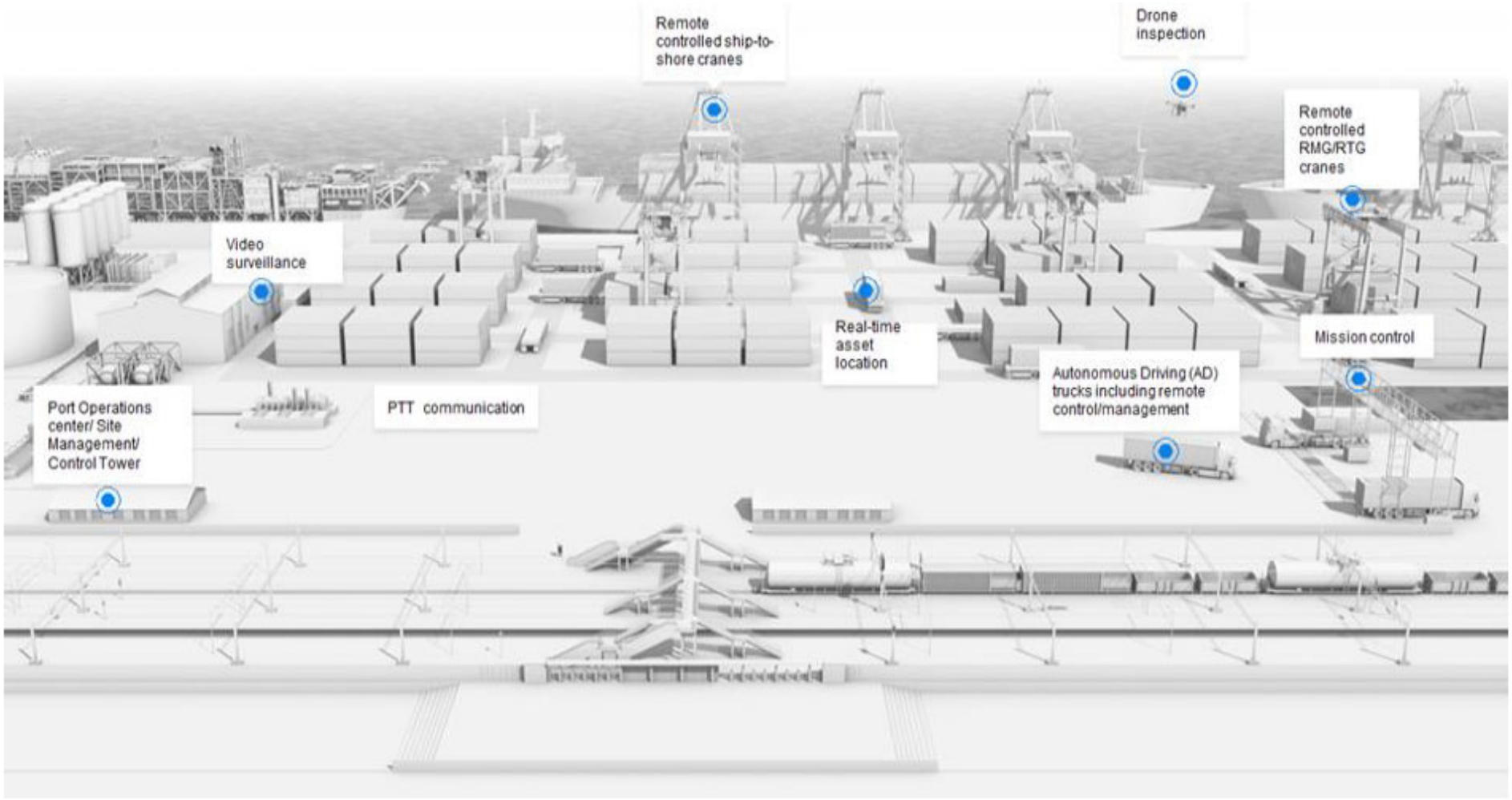
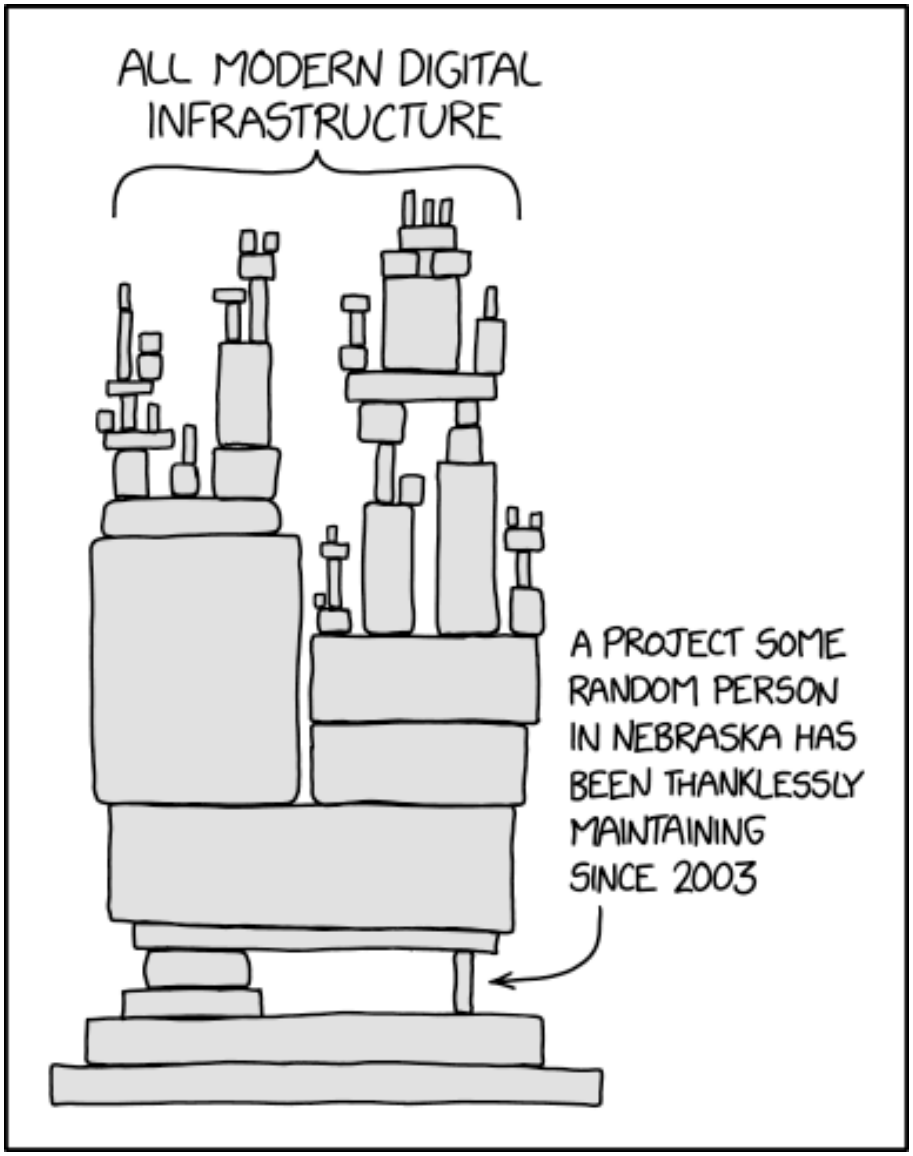



**FIGURE 3. SMART PORT USE CASES**

# 5G als militärisches Risiko

- Präzise Ortung von 5G-fähigen Objekten und deren Bewegung:
  - Transportsysteme, Waffensysteme
  - Mobile Versorgungs- und Kommandostrukturen
  - Warenlieferungen (Schiffe, Häfen, Flugplätze, Warenlager etc.)
  - …
- Störung der Abläufe und Unterbruch von Versorgungsketten
- Vorhersage zukünftiger Aufenthaltsorte für kinetische Zugriffe
- Einspeisung / Verfälschung von Informationen und Denial of Service
- Ableitung taktischer und/oder strategischer Planungsinformationen






NEWS

Über 350'000 betroffene Projekte

# 15 Jahre alte Schwachstelle gefährdet zigtausende Open-Source-Projekte

Di 27.09.2022 - 12:23 Uhr
von Yannick Züllig und aob

Ein seit 15 Jahren ungepatchte Schwachstelle eines Python–Moduls gefährdet über 350'000 Open-Source-Projekte. Angreifer können die Schwachstelle nutzen, um beliebigen Code auf der betroffenen Maschine auszuführen.

| Name | Description | Risk Level |
| --- | --- | --- |
| Binary-Artifacts | Is the project free of checked-in binaries? | High |
| Branch-Protection | Does the project use Branch Protection ? | High |
| CI-Tests | Does the project run tests in CI, e.g. GitHub Actions, Prow? | Low |
| CII-Best-Practices | Does the project have a CII Best Practices Badge? | Low |
| Code-Review | Does the project require code review before code is merged? | High |
| Contributors | Does the project have contributors from at least two different organizations? | Low |
| Dangerous-Workflow | Does the project avoid dangerous coding patterns in GitHub Action workflows? | Critical |
| Dependency-Update-Tool | Does the project use tools to help update its dependencies? | High |
| Fuzzing | Does the project use fuzzing tools, e.g. OSS-Fuzz? | Medium |
| License | Does the project declare a license? | Low |
| Maintained | Is the project maintained? | High |
| Pinned-Dependencies | Does the project declare and pin dependencies? | Medium |
| Packaging | Does the project build and publish official packages from CI/CD, e.g. GitHub Publishing ? | Medium |
| SAST | Does the project use static code analysis tools, e.g. CodeQL, LGTM, SonarCloud? | Medium |
| Security-Policy | Does the project contain a security policy? | Medium |
| Signed-Releases | Does the project cryptographically sign releases? | High |
| Token-Permissions | Does the project declare GitHub workflow tokens as read only? | High |
| Vulnerabilities | Does the project have unfixed vulnerabilities? Uses the OSV service. | High |

# OSSARA: Abandonment Risk Assessment for Embedded Open Source Components

Xiaozhou Li, Sergio Moreschini, Fabiano Pecorelli, and Davide Taibi, Tampere University

*// Systems with unmaintained embedded open source software (OSS) components are vulnerable to severe risks. This article introduces the OSS Abandonment Risk Assessment model to help companies avoid potentially dire consequences. //*

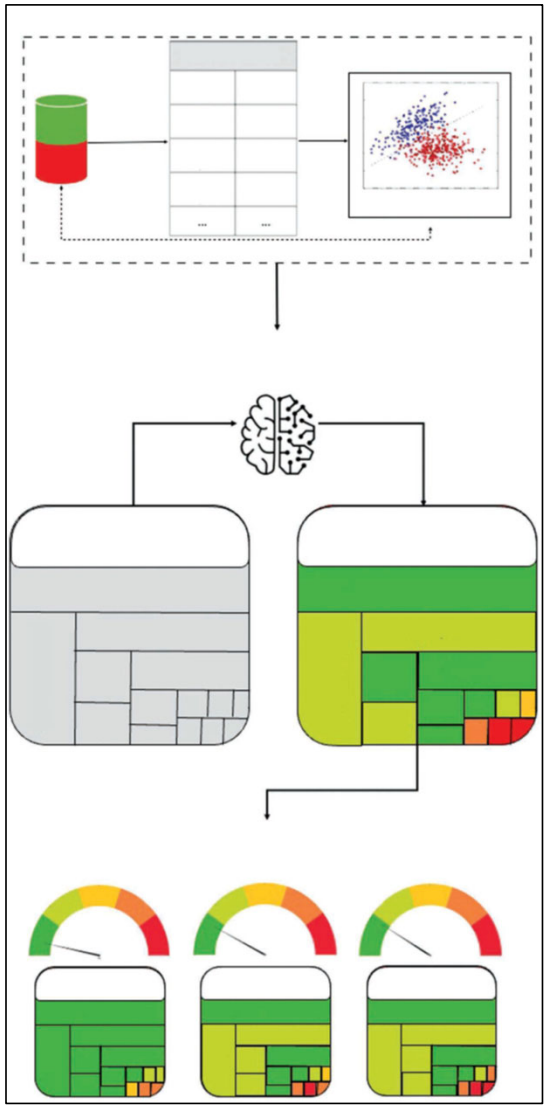
**SOFTWARE NEEDS TO** be continuously updated and maintained to continue being useful.[1] This is particularly true for open source software (OSS) components and libraries, which are more and more often integrated into large and complex systems. For companies developing long-term projects, all embedded OSS components should guarantee lengthy life expectancies and be maintained as long as systems are in service. Embedding abandoned OSS in critical systems could expose companies to severe risks. For example, new security vulnerabilities could be exploited, bugs and issues might never be resolved, and functions could become obsolete and inadequate for new environments. Metaphorically, systems embedding abandoned OSSs are like vehicles with rusted gears or human bodies with malignant tumors. Indeed, the abandonment of OSS components might produce a "domino effect" that results in the inoperability of full systems. The importance of such a statement is in the fact that even if a single embedded software component is unavailable, a whole project can be compromised.

In this respect, we were recently asked by a local branch of a global company, which operates in different domains and with more than 200,000 employees in 150-plus countries, to devise a methodology aimed at identifying components embedded in its software products that were the most likely to be abandoned soon. To meet the requirements, we designed the OSS Abandonment Risk Assessment (OSSARA) model, which we present in this article. The model aims to assess the abandonment risk of a software system through prediction for every embedded OSS component and the criticality that each component represents. With OSSARA, practitioners can monitor a system's risk level and choose to maintain or replace OSS components.

## Related Work

During the past decade, researchers have been paying great attention

*Digital Object Identifier 10.1109/MS.2022.3163011*
*Date of current version: 20 June 2022*



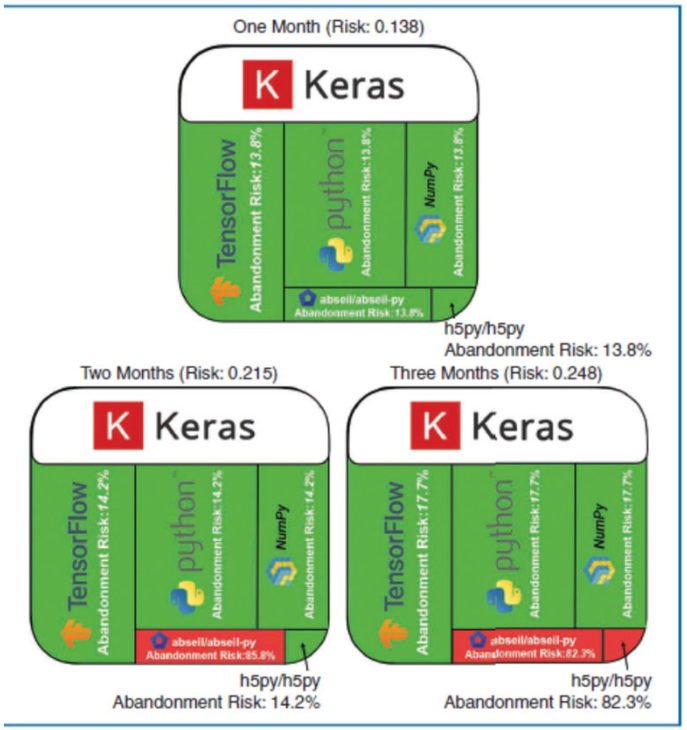



**FIGURE 2.** The abandonment risk assessment for Keras.


"Try switching it off and on at the same time."

# Das «Quantenversum»

- Quantum Computing – mehr parallelisierte Rechenleistung für ausgewählte Teilprobleme (Spezial-Algorithmen) mit erheblichen Auswirkungen auf die traditionelle, nicht beweissichere Chiffrierung usw.
- Quantum Internet –
  - Neue Protokolle (Quantum Teleportation, Quantum Coding etc.)
  - Neue Netzwerkstrukturen (Parallelisierung durch Quanten-Repeater/Switches etc.)
  - Quantenchiffrierung

- Quantensichere (Postquantum) Chiffrierung – NIST hat die vier Gewinner der öffentlichen Wettbewerbs benannt

# Drei Kategorien von Quantenalgorithmen

- Algorithmen, die auf der Quanten-Fouriertransformation beruhen, z.B. der Shor-Algorithmus zur Faktorisierung großer ganzer Zahlen, der für die Primzahlzerlegung in der Kryptographie eine wichtige Rolle spielt.
- Quanten-Suchalgorithmen, z.B. der Grover-Algorithmus (mit Varianten) zur effizienten Suche in einem unsortierten Array. Bei n Einträgen im Array braucht ein klassischer Computer maximal n Rechenschritte, ein Quantencomputer $\sqrt{n}$.
- Quanten-Simulation (z.B. Quantenchemie) durch einen geeigneten Satz von Quantengattern in einer Quantenschaltung, die alle Hamilton-Operatoren (ein Operator der Quantenmechanik, der (mögliche) Energiemesswerte und die Zeitentwicklung darstellen kann.
- Aber: ein sehr erheblicher Teil der parallelisierten Rechenleistung wird für die interne Fehlerkorrektur benötigt.

# Quantenchiffrierung

- Ziel: Es können zwei Instanzen gemeinsam einen digitalen Schlüssel erstellen, den keine andere Person unbemerkt mitlesen kann.
- BB84 Protokoll zum Quantenschlüsselaustausch mittels Photonen, die je nach ihrer Polarisation bzw. ihrem Spin (Drehrichtung) einen Teil des Schlüssels repräsentieren.
- Werden Photonen unterwegs abgefangen / gemessen, ändert sich ihr «Spin», d.h. der Empfänger weiss, dass der Schlüsselaustausch mitgelegen und ggf. kompromittiert wurde (Hintergrund: die Gesetze der Quantenmechanik verbieten bzw. verunmöglichen eine beliebig genaue Messung aller möglichen Polarisationsrichtungen zur gleichen Zeit).

# Quantensichere (Postquantum) Chiffrierung

- Mehrheit der vier Gewinner-Algorithmen (einer für Chiffrierung, drei für digitale Signaturen) sind Gitterverfahren.
  - In einem 2-dimensionalen Raum werden zur Definition eines Gitters zwei Vektoren benötigt (Basisvektoren). Die Gitterpunkte sind dann die positiven oder negativen Vielfachen der Basisvektoren.
    Die Wege von der Basis zu den anderen Gitterpunkten bzw. der kürzeste Weg von einem Gitterpunkt P zur Basis als Grundlage einer Entschlüsselung lassen sich zwar durch Quantencomputer auch stark parallelisiert berechnen, aber wenn man die Dimensionen des Raums stark erhöht (z.B. 500 Dimensionen = $2^{500}$ Gitternachbarn = eine Zahl mit 150 Stellen), reicht auch die Rechenleistung eines Quantencomputers nicht aus.
- Vier weitere Verfahren (asymmetrische Chiffrierverfahren ohne Gitterverfahren, mit fehlerkorrigierenden Codes und sehr (zu) langen Schlüsseln) sind für eine nächste Runde nominiert – einer davon (SIKE) auf Basis elliptischer Kurven wurde inzwischen erfolgreich attackiert und ist in Gefahr, auszuscheiden.
- Aber: sehr langsame Umsetzung und Eingang in Software und Hardware Produkte und nur langsame Verdrängung der «legacy» RSA- und RSA-ähnlichen Systeme

# Und endlich …

IT INSIDE IT

INSERIEREN JOBPORTAL INSIDE CHANNELS FORUM

TECHNOLOGIE PARTNER

DEEPIMPACT

GOLD SPONSOREN

## Edöb: "Vertrauen Behörden nur auf private Gutachten, können sie sich eine blutige Nase holen"

Von Thomas Schwendener, 28. September 2022 um 13:41

POLITIK & WIRTSCHAFT EDÖB DATENSCHUTZ CLOUD E-GOVERNMENT JUSTIZ



EDÖB Adrian Lobsiger: "Ich bin mir bewusst, dass wir vor einem Dilemma stehen."

**Der Eidgenössische Datenschützer kritisiert Anwaltskanzleien, die Behörden beim Einsatz von US-Cloud-Diensten Sicherheit versprechen. Im Interview schildert Adrian Lobsiger seine Sicht.**

# Und immer noch / immer wieder …

**Nationale Cyberstrategie (NCS)**

Fazit:
alte Probleme bleiben,
neue kommen dazu