

IBM “5 in 5” 2018

—
Thomas Landolt
Managing Director IBM

5 in 5

Five innovations that will help change
our lives within five years

The IBM logo, consisting of the letters "IBM" in a bold, sans-serif font, is positioned in the bottom right corner of the blue rectangular area.

What is the 5 in 5?

Each year, we showcase some of the biggest breakthroughs coming out of IBM Research's global labs – five technologies that we believe will fundamentally reshape business and society in the next five years.



Why here?

All the technologies presented in the "5 in 5" impact society in one or the other way.

At IBM, we use this to direct future focus for research which also drives a long term view on investments. The same needs to be done for Defense & Intelligence organizations.

Imagine a Defense & Intelligence organization that delivers ...



Outstanding Mission Outcomes
across critical domains



Defense platforms



Logistics



Cyber Security



"Open" Source
Intelligence



Command, Control
and Communications

IBM

Defense and Intelligence agencies face an array of challenges and technology constraints

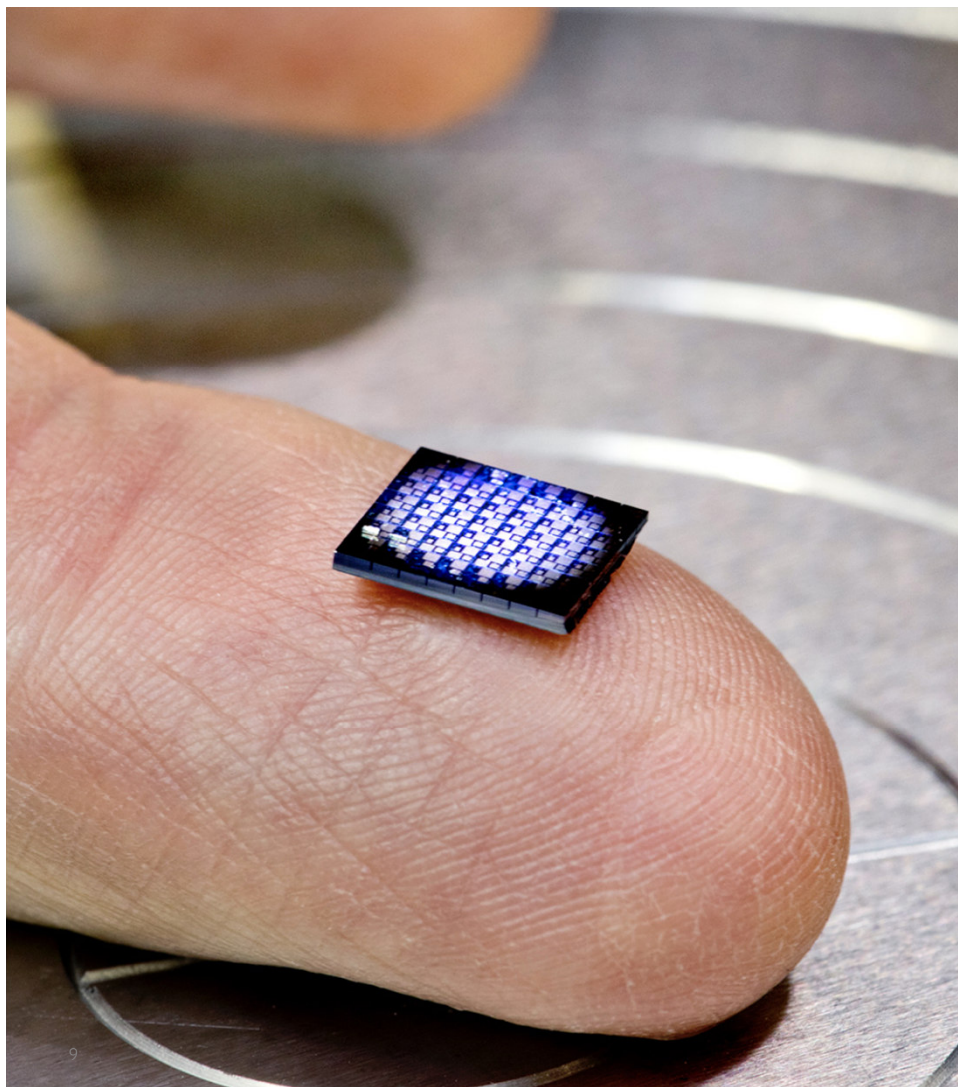


Nobody likes knockoffs.
Crypto-anchors and
blockchain will unite
against counterfeiters.







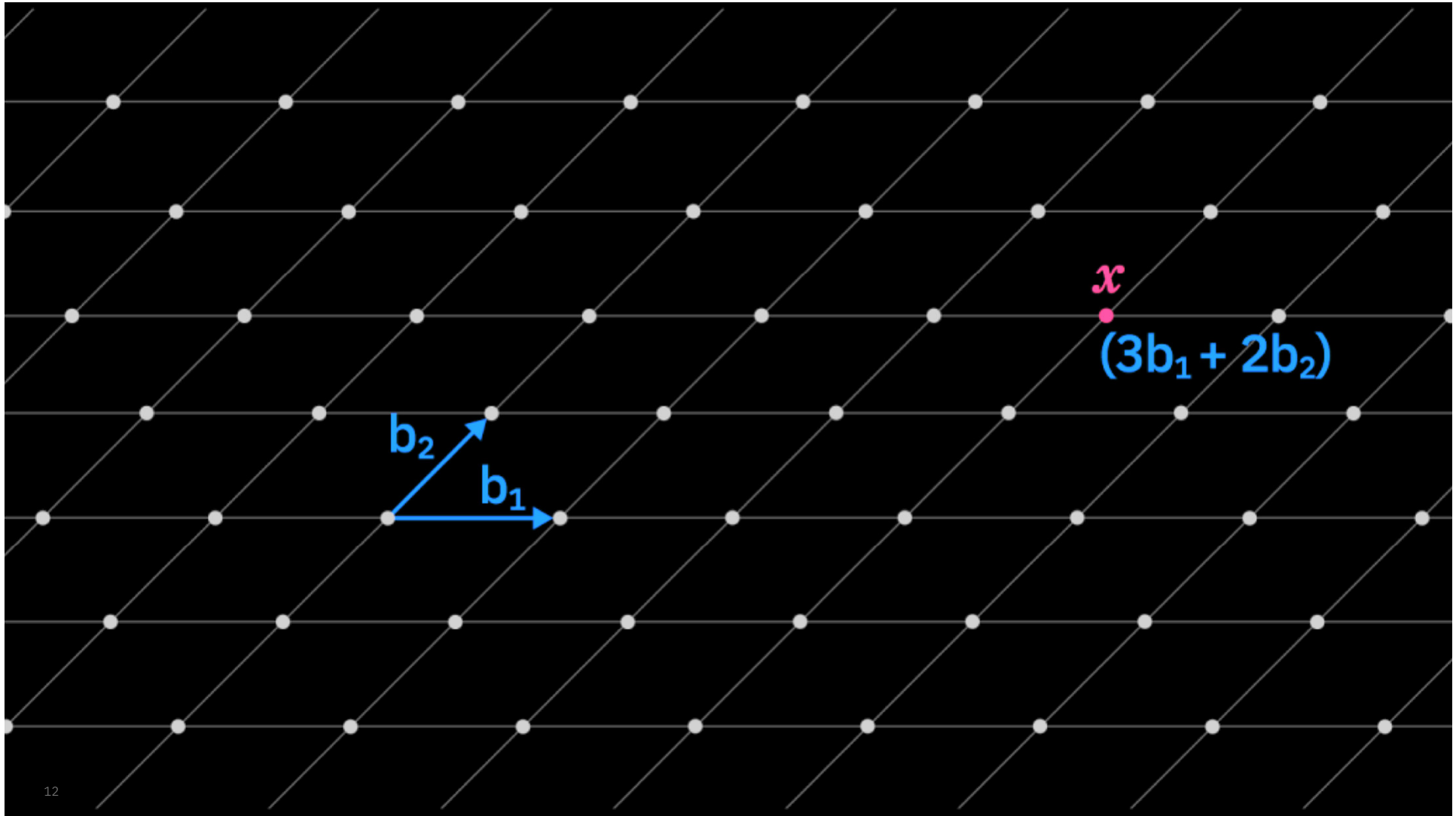


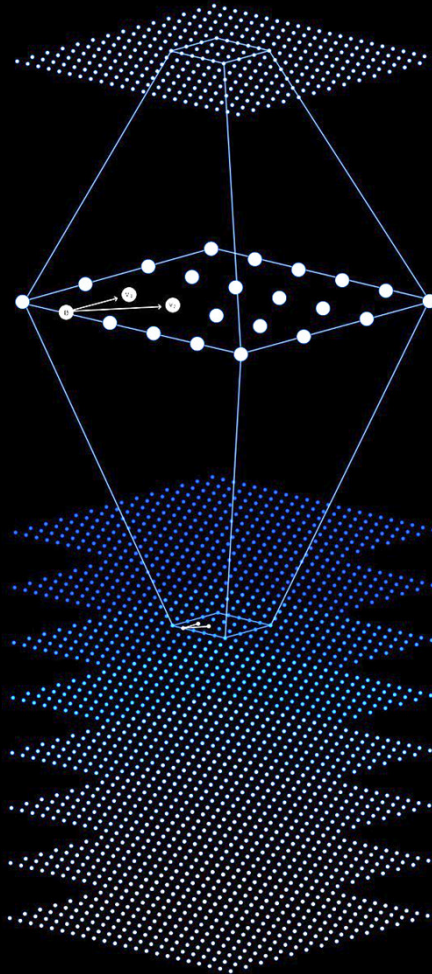
... and its Applicability in Defense & Intelligence

- Guaranteed provenance of spare parts management to improve service delivery time, quality and cost.
- Establish a distributed management system to know location, configuration and readiness status of all your assets.
- Operate on a cost effective, flexible and mobile modern infrastructure, from headquarters to deployed, trusted across a network of organizations.
- Establish a safe and fair method to take care of the displaced and paperless and preventing the infiltration of individuals who are known security threats.
- Improve co-operation between multiple parties to allow for seamless joint operations.

Hackers gonna hack. Until they encounter lattice cryptography.



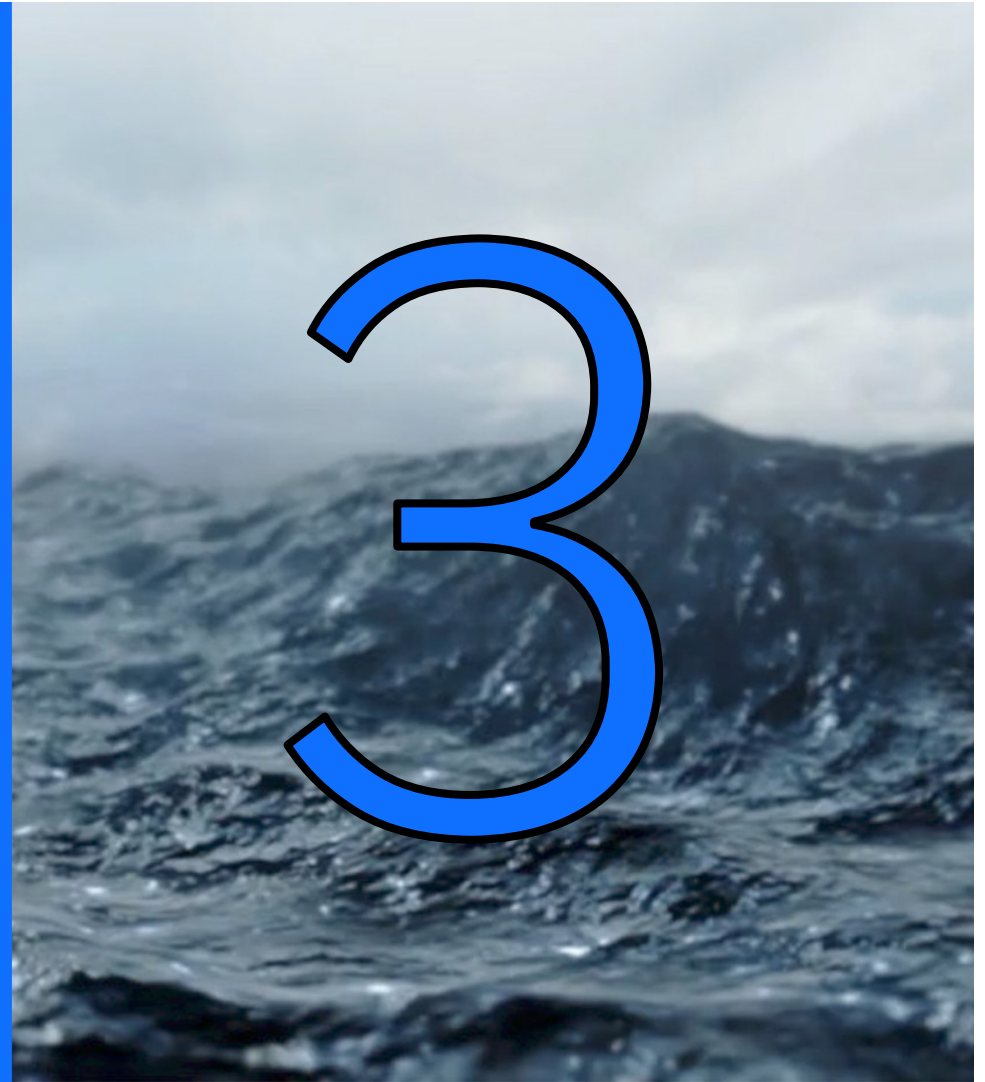


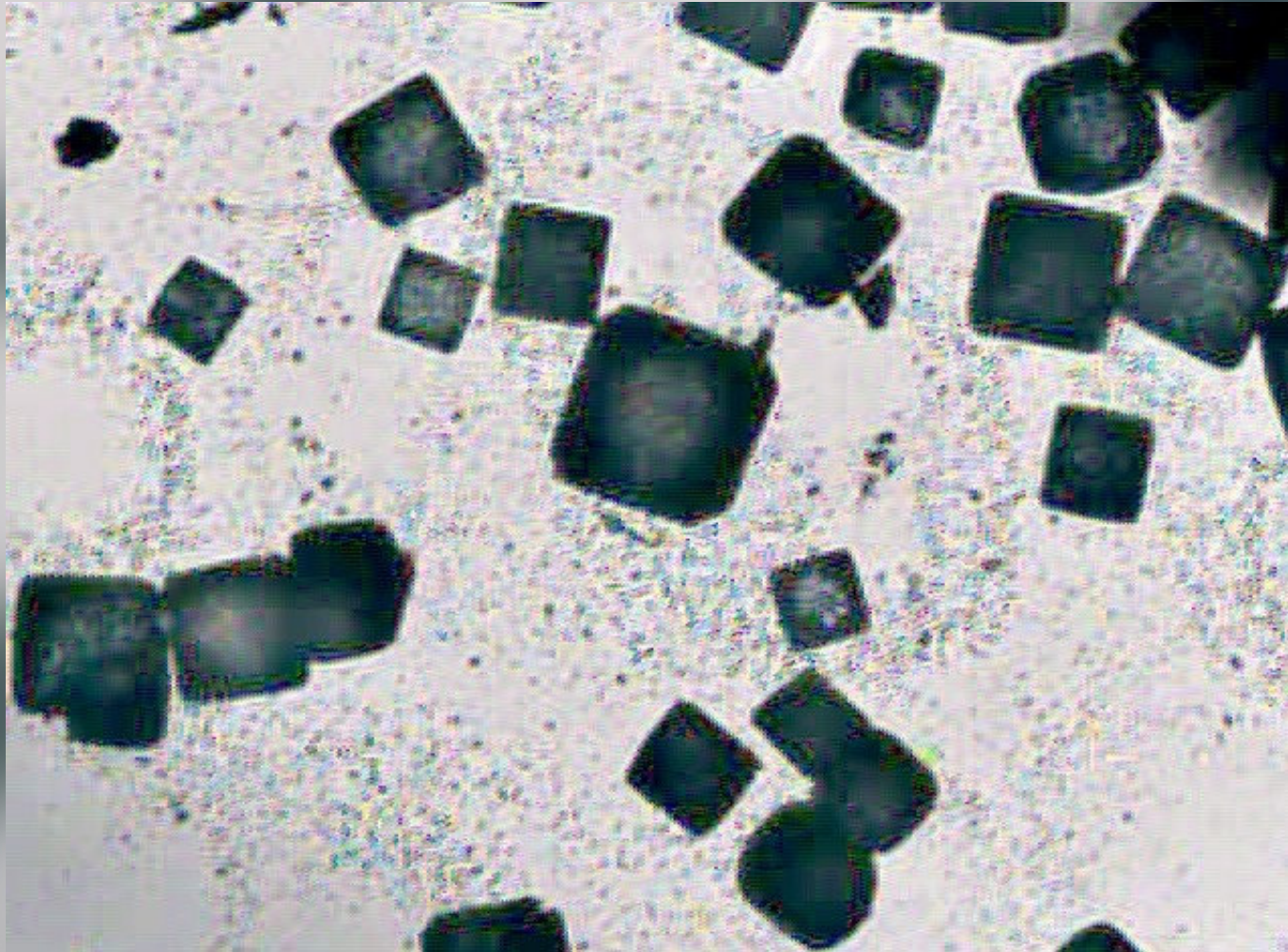


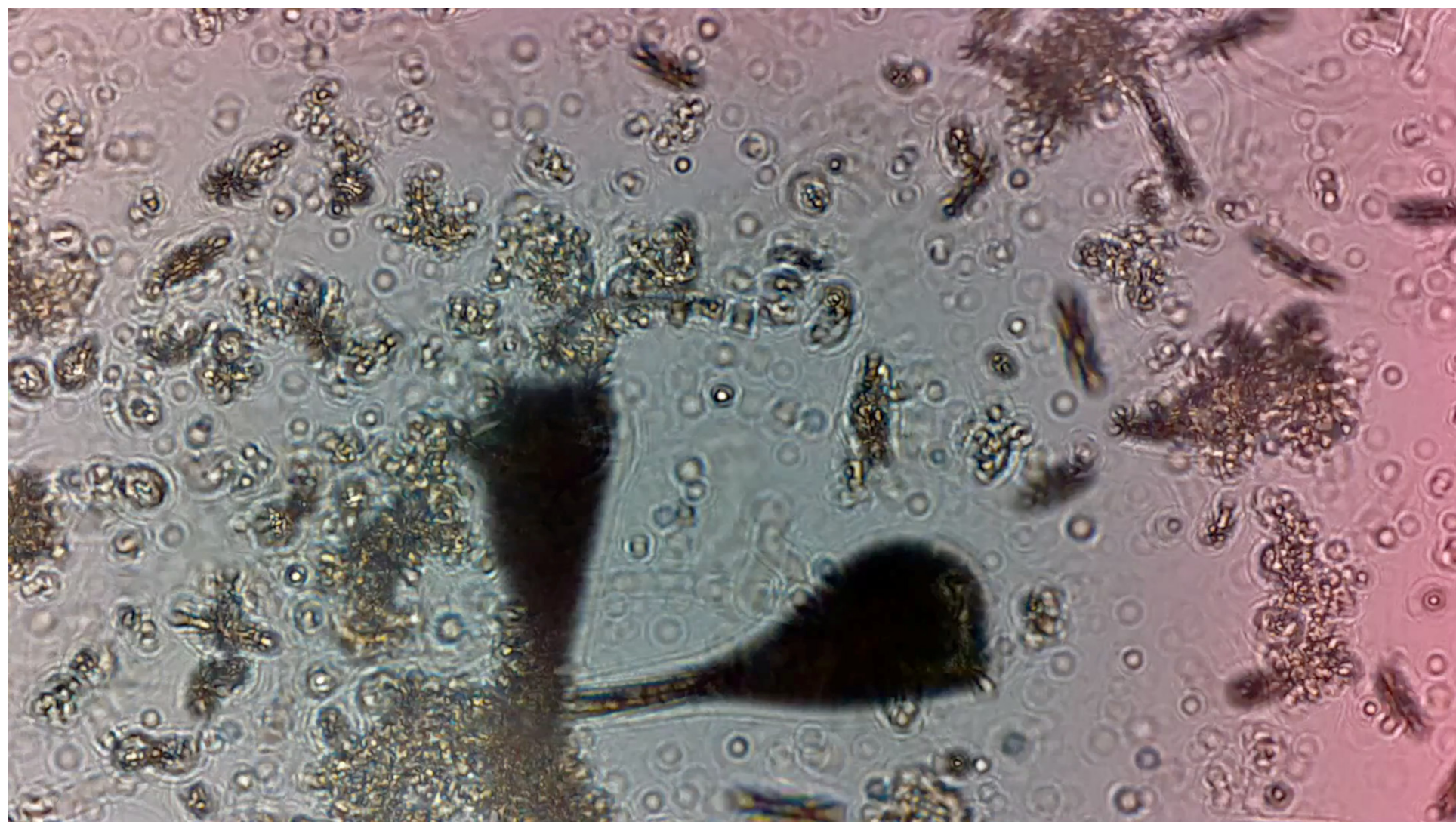
... and its Applicability in Defense & Intelligence

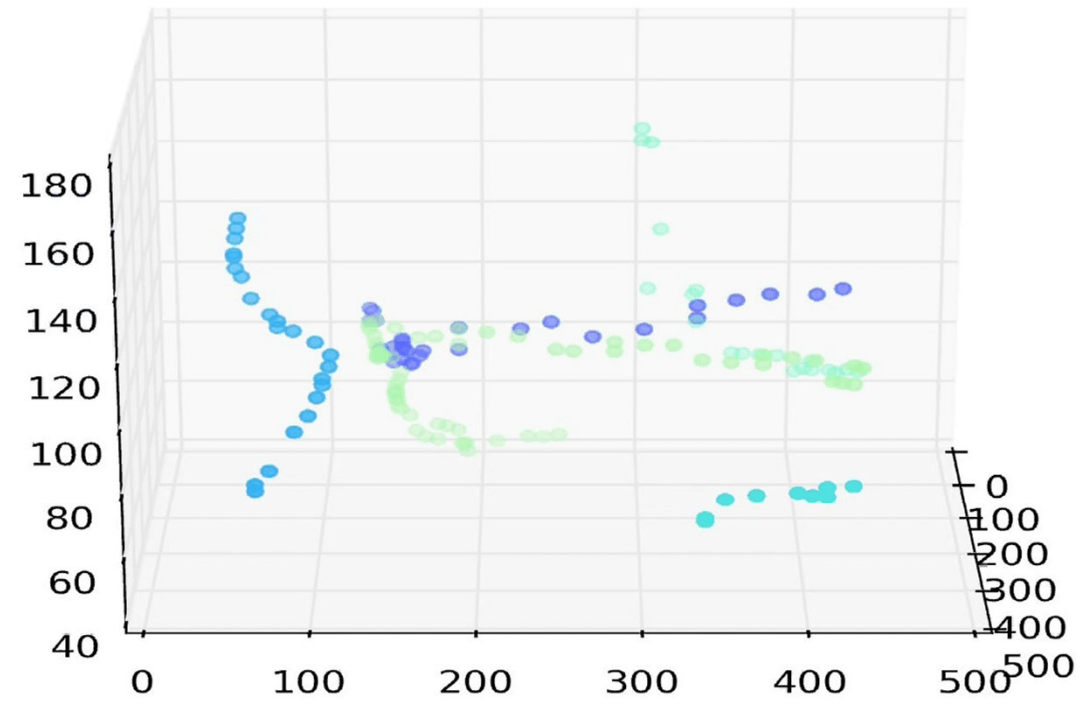
- While the first Quantum decryption algorithms are still a few years away, changing the encryption of large and possibly distributed archives is costly and time consuming.
- New encryption methods will have to be deployed and used across the whole network of allies.
- Encryption has to fit with an overall concept against cyber threats.

Our oceans are dirty. AI-powered robot microscopes may save them.









... and its Applicability in Defense & Intelligence

- Real time monitoring of critical resources such as water but also air to predict various threats.
- Deployment of AI enabled sensors, which are autonomous and durable into the field for surveillance and reconnaissance

AI bias will explode. But
only the unbiased AI will
survive.

4



Continued influence effect

The tendency to believe previously learned misinformation even after it has been corrected. Misinformation can still influence inferences one generates after a correction has occurred.

Google effect

Remembering to forget information that can be looked up online by using Internet search engines.

Duration neglect

The neglect of the duration of an episode in determining its value.

Mere exposure effect

The tendency to express undue liking for things merely because of familiarity with them.

Cross-race effect

The tendency for people of one race to have difficulty identifying members of a race other than their own.

Denomination effect

The tendency to spend more money when it is denominated in small amounts rather than large.

Stereotyping

Expecting a member of a group to have certain characteristics without having information about that individual.

Third-person effect

Belief that one's communication efforts will have more influence on others than on oneself. The results of a joint action are more likely to be credited to the other person than an outside observer would credit.

Attentional bias

The tendency of our perception to be influenced by our recurring concerns.

Automation bias

Automation bias is a cognitive bias that occurs when we rely too heavily on automated systems or algorithms, even when we have information that contradicts or refutes their output. This can lead to errors in judgment and decision-making.

Backfire effect

When someone is presented with disconfirming evidence by a source they trust, they may actually strengthen one's previous belief.

Egocentric bias

Belief that one's communication efforts will have more influence on others than on oneself. The results of a joint action are more likely to be credited to the other person than an outside observer would credit.

Choice-supportive bias

The tendency to remember choices as better than they actually were.

Surrogate

Loss of sight of the strategic construct that a measure is intended to represent, and subsequently acting as if the measure is the construct of interest.



... and its Applicability in Defense & Intelligence

- AI systems and algorithms will become widely used in Defense & Intelligence scenarios. E.g.: bias can lead to wrong situation assessments.
- Applications for AI: Scenario planning, command support, information analysis, social media analysis, face and vision analysis, video stream analysis
 - for all those applications it's critical to develop and train these systems with data that is fair, interpretable and free of racial, gender, or ideological biases.

Today, quantum computing is a researcher's playground. In five years, it will be mainstream.







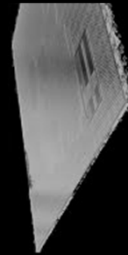
... and its Applicability in Defense & Intelligence

- Possible applications for Quantum Computing are Complex Simulations, Code Decryption, Systems Analysis, Material Science, Supply Chain & Logistics, Machine Learning – all highly relevant for Defense & Intelligence.
- Quantum Computers will eventually surpass the capabilities of classical computers for specific problems.

5 in 5

Five innovations that will help change our lives within five years

1 - Nobody likes knockoffs. Crypto-anchors and blockchain will unite against counterfeiters.



2 - Hackers gonna hack. Until they encounter lattice cryptography.



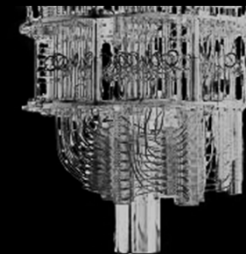
3 - Our oceans are dirty. AI-powered robot microscopes may save them.



4 - AI bias will explode. But only the unbiased AI will survive.



5 - Today, quantum computing is a researcher's playground. In five years, it will be mainstream.



IBM

Additional resources

Changing the way the world works: IBM Research's "5 in 5"

Blog by Arvind Krishna, Head of IBM Research

<https://www.ibm.com/blogs/research/2018/03/ibm-research-5-in-5-2018/>

IBM Research 5 in 5 website

<https://www.research.ibm.com/5-in-5/>

5 in 5 video playlist

<https://bit.ly/2GtPOwZ>

5 in 5 Science Slam at Think 2018

<https://www.ibm.com/events/think/watch/replay/113720903/>



IBM