



THE RED (TEAM) ANALYSIS SOCIETY

Quantum Computing, Geopolitical Stakes and Impacts - The Quantum Battlefield and the Future

Helene Lavoix

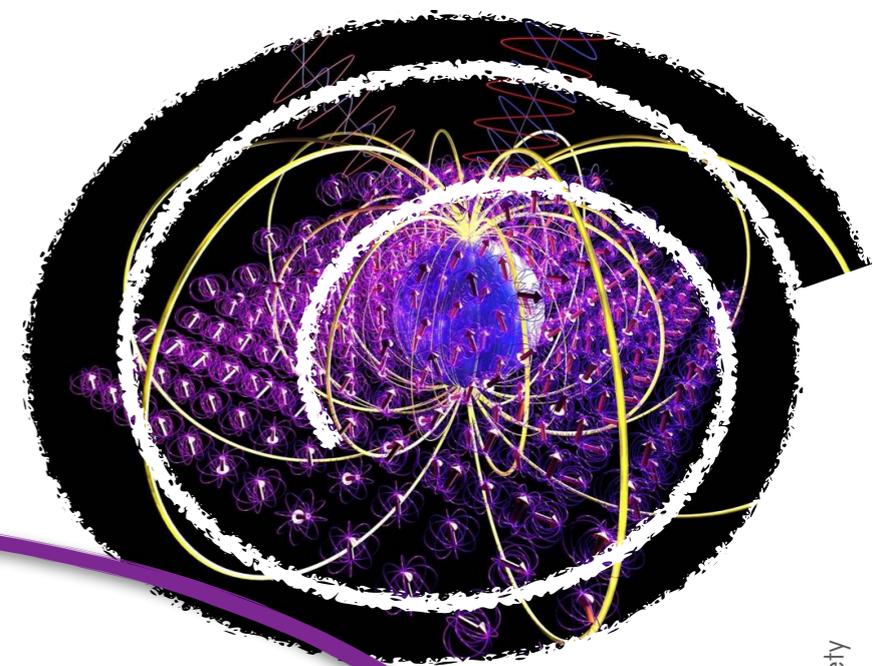
30 November 2018 v2 - pdf version

International Conference on Quantum Computing
ICoQC 2018
Ecole Normale Supérieure, Paris, France
26 - 30 November 2018

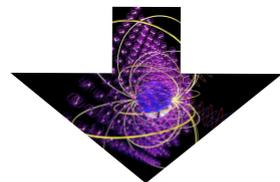
Nota for the pdf version

- Some illustrative images have been removed.
- The videos cannot be included in the pdf version and thus have been removed.
- (Obviously) animations have been removed.
- A biography has been added at the end.

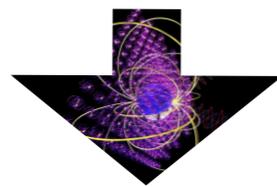
Why does it matter to look at future (security) impacts?



Science and Engineering Findings



1 Imagining the Quantum AI world (with evidence + security stakes)

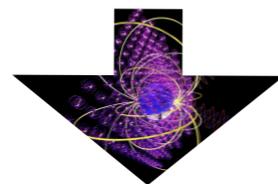


Stakeholders with varying interests and thus actions...

2

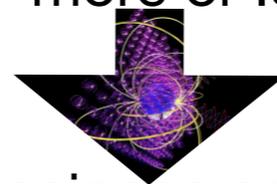
- Scientists - discoveries, funding and various self interest
- States/political authorities - power (influence, resources (taxes)) and security
- Companies/industries - future clients and markets and threat to their survival

=> The race to quantum



3

Different aims + international milieu → more or less tension among actors → impact on the race.



Means + actions on the race impacts science and application, which in turn impacts both the actualisation of what was foreseen and further imagination.

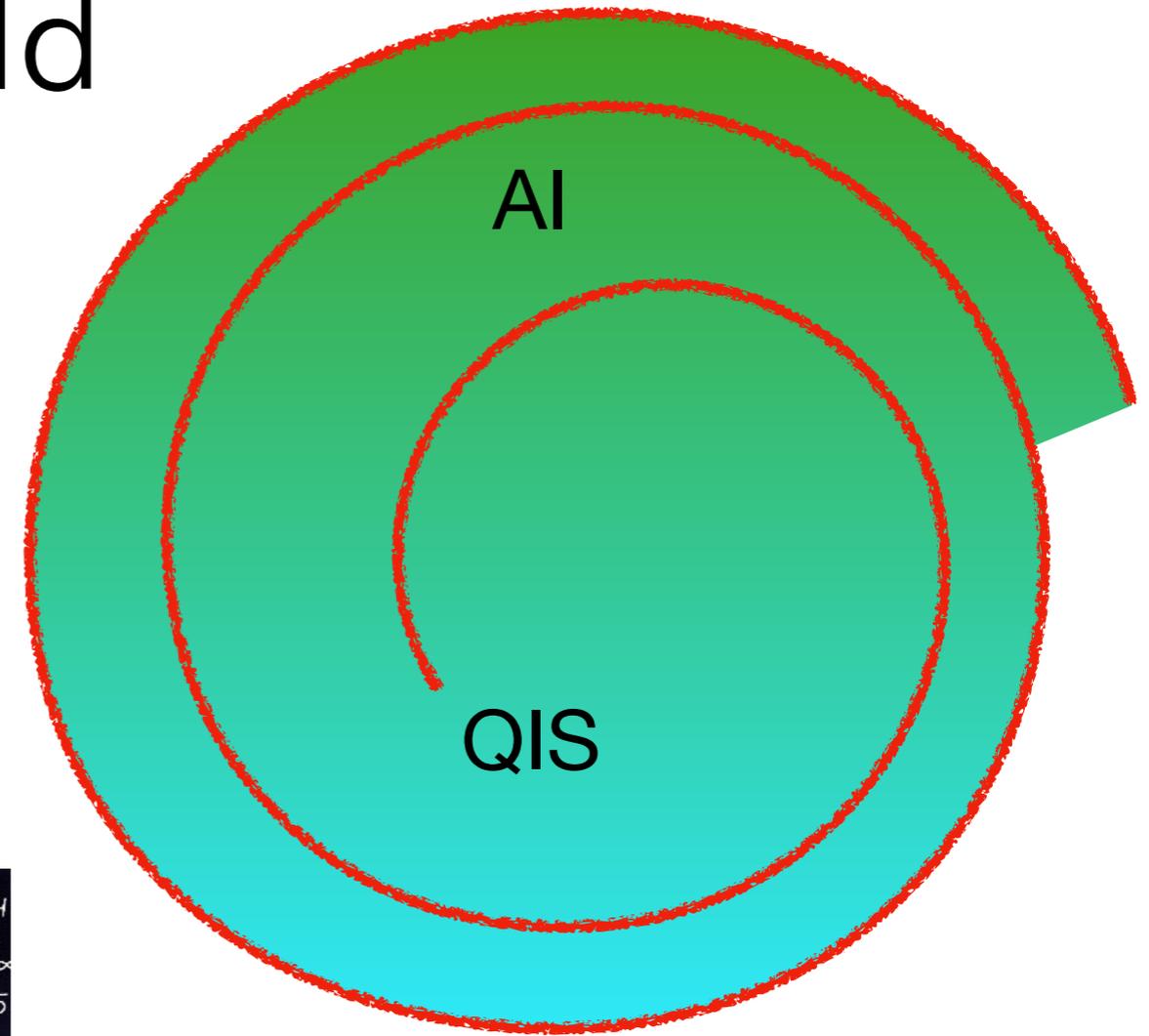
Image: AFRL-supported physicists at the University of Michigan (UM) are developing innovative components for quantum (Artistic rendering by UM Applied Physics doctoral student Bo Sun)

1 The Emerging Future Quantum- AI World and Security Stakes



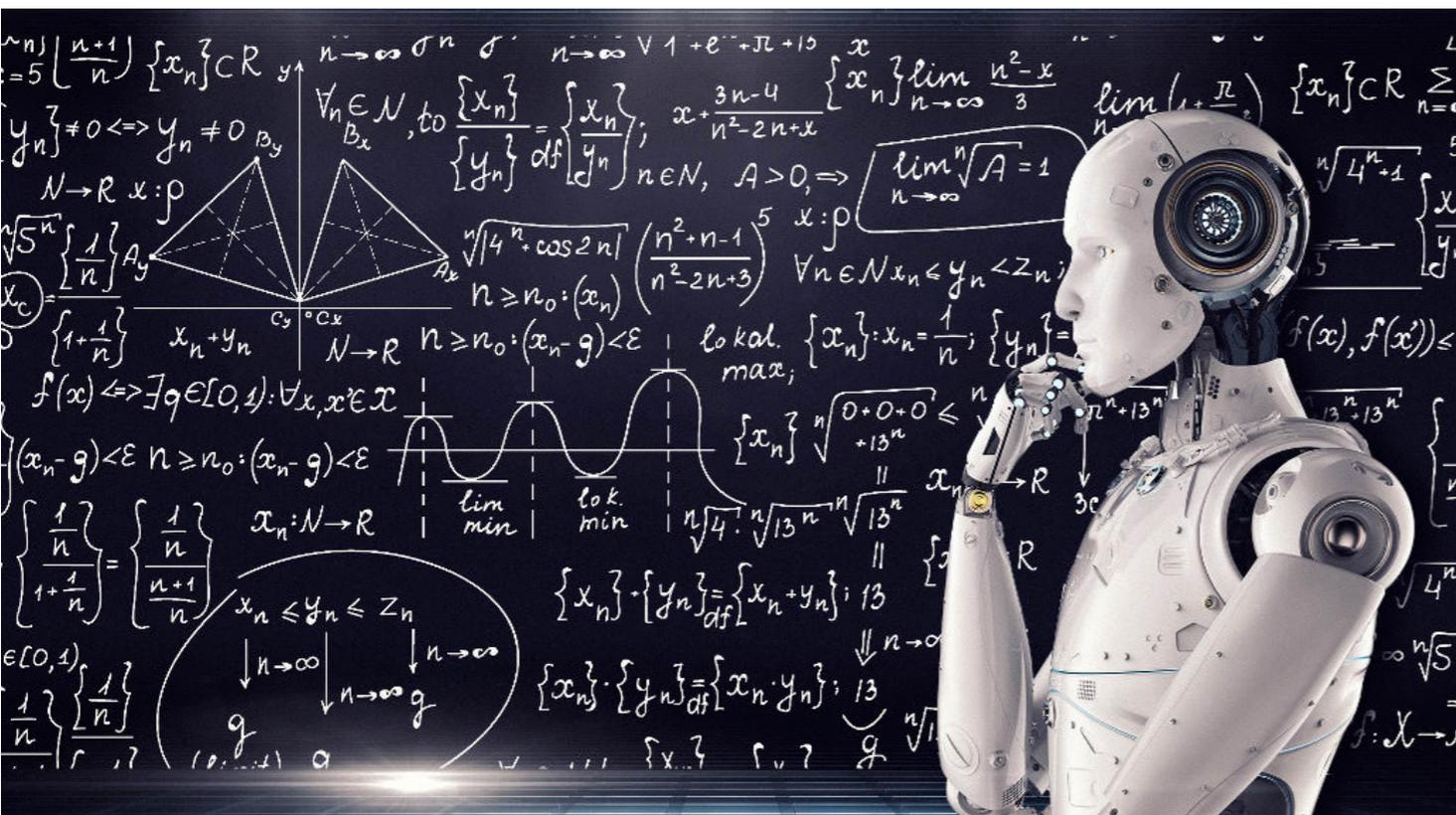
Towards a Future Quantum-AI World

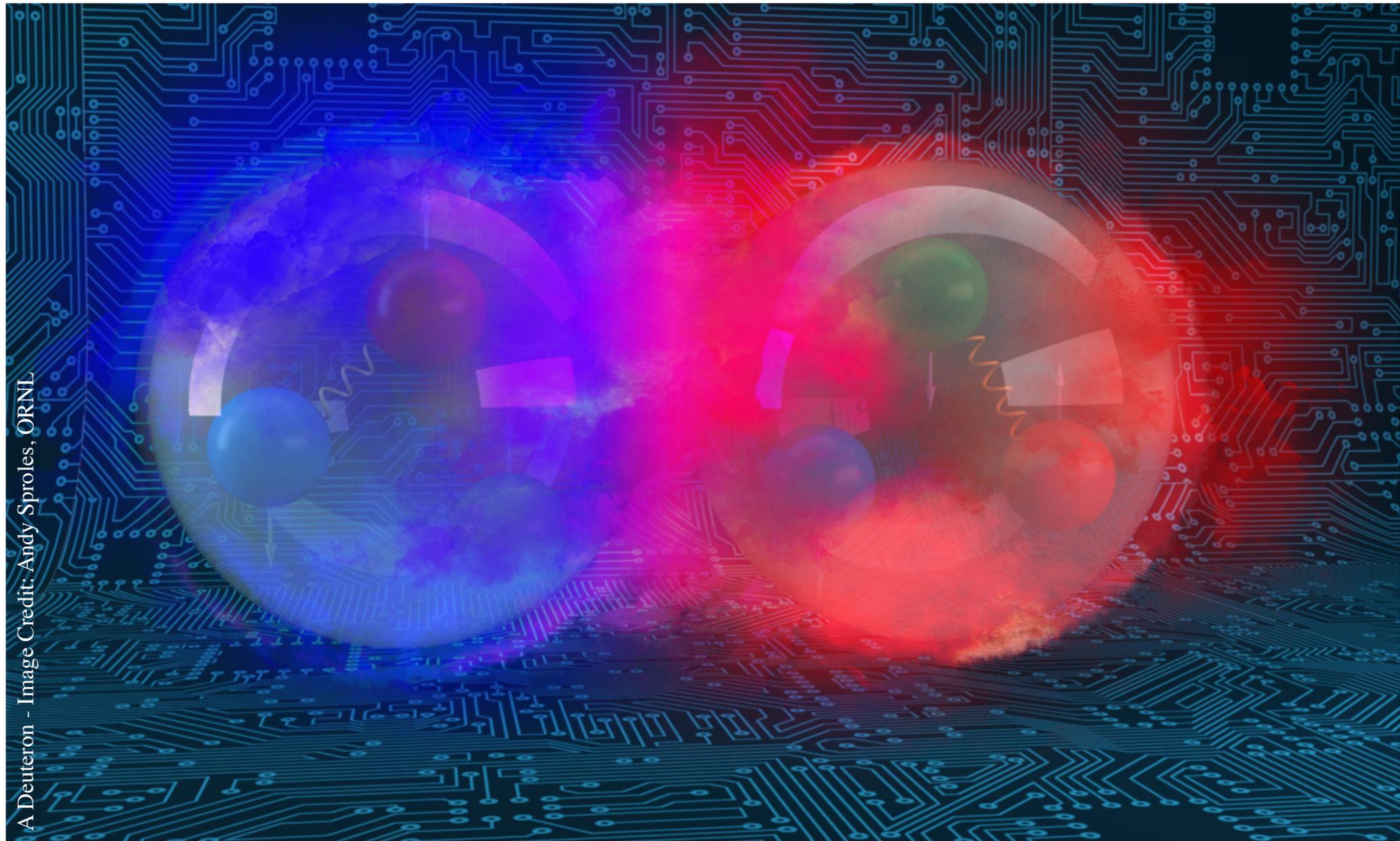
- QIS benefits from AI and changes AI
- AI benefits QIS and allows for evolution



Escalating feedback loop between QIS and AI

e.g. The “quantum perceptron” (Francesco Tacchino, Chiara Macchiavello, Dario Gerace, Daniele Bajoni, “An Artificial Neuron Implemented on an Actual Quantum Processor”, [arXiv:1811.02266](https://arxiv.org/abs/1811.02266) , 6 Nov 2018)





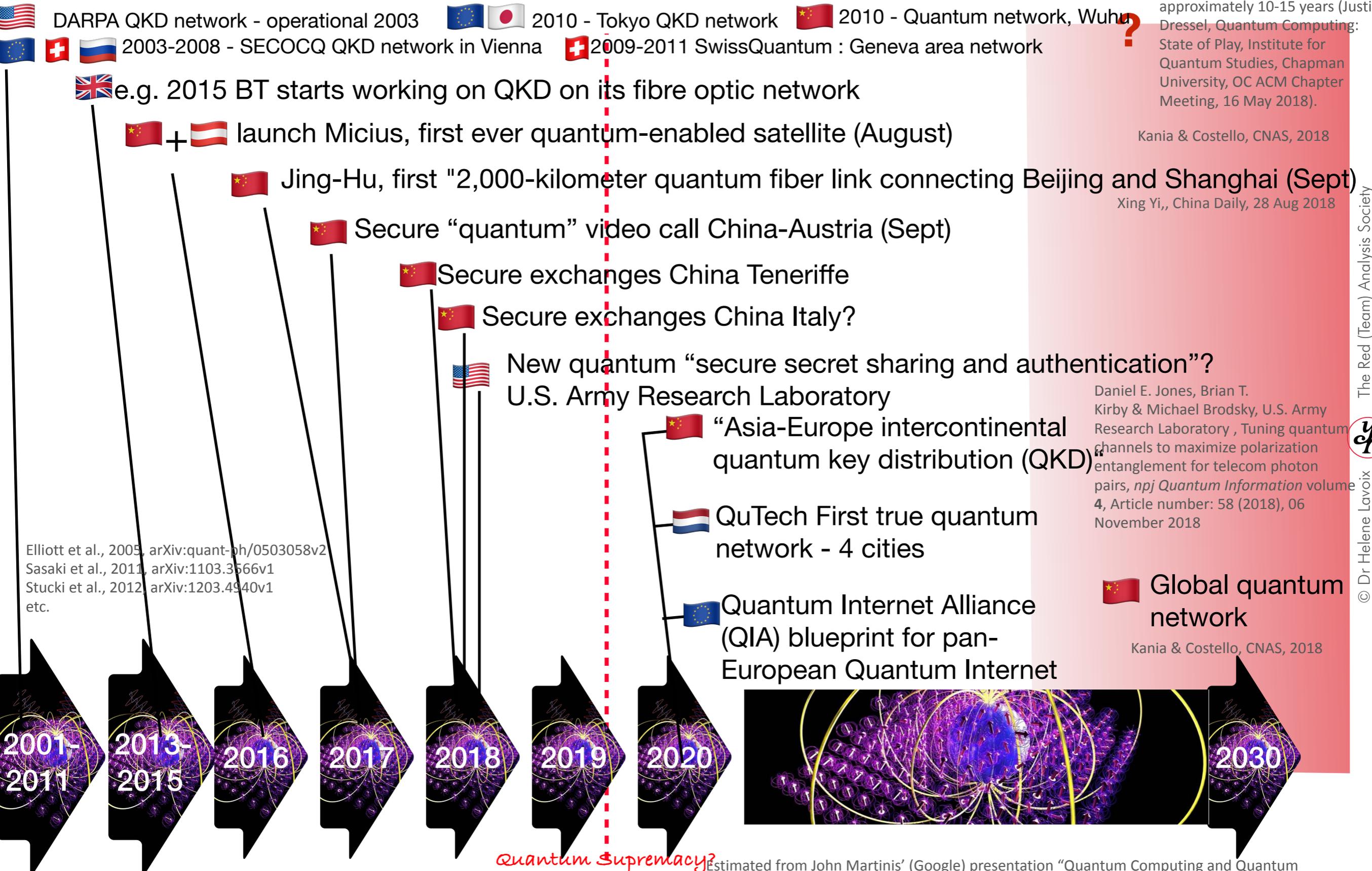
A Deuteron - Image Credit: Andy Sproles, ORNL

Countering a Quantum Computing “Crypto-apocalypse”

Quantum Communication & cryptography: getting very
secure communications

Countering the Perceived Possibility of a Quantum Computing "Crypto-apocalypse"

Various Field Trials (non exhaustive)



Chips with one billion qubits in approximately 10-15 years (Justin Dressel, Quantum Computing: State of Play, Institute for Quantum Studies, Chapman University, OC ACM Chapter Meeting, 16 May 2018).

Kania & Costello, CNAS, 2018

Xing Yi,, China Daily, 28 Aug 2018

Daniel E. Jones, Brian T. Kirby & Michael Brodsky, U.S. Army Research Laboratory , Tuning quantum channels to maximize polarization entanglement for telecom photon pairs, *npj Quantum Information* volume 4, Article number: 58 (2018), 06 November 2018

Global quantum network

Kania & Costello, CNAS, 2018

Quantum Supremacy?

Estimated from John Martinis' (Google) presentation "Quantum Computing and Quantum Supremacy" (HPC user Forum, Tuscon, April 16-18, 2018) / Pan Jianwei plans for 2020

Countering Quantum Computing

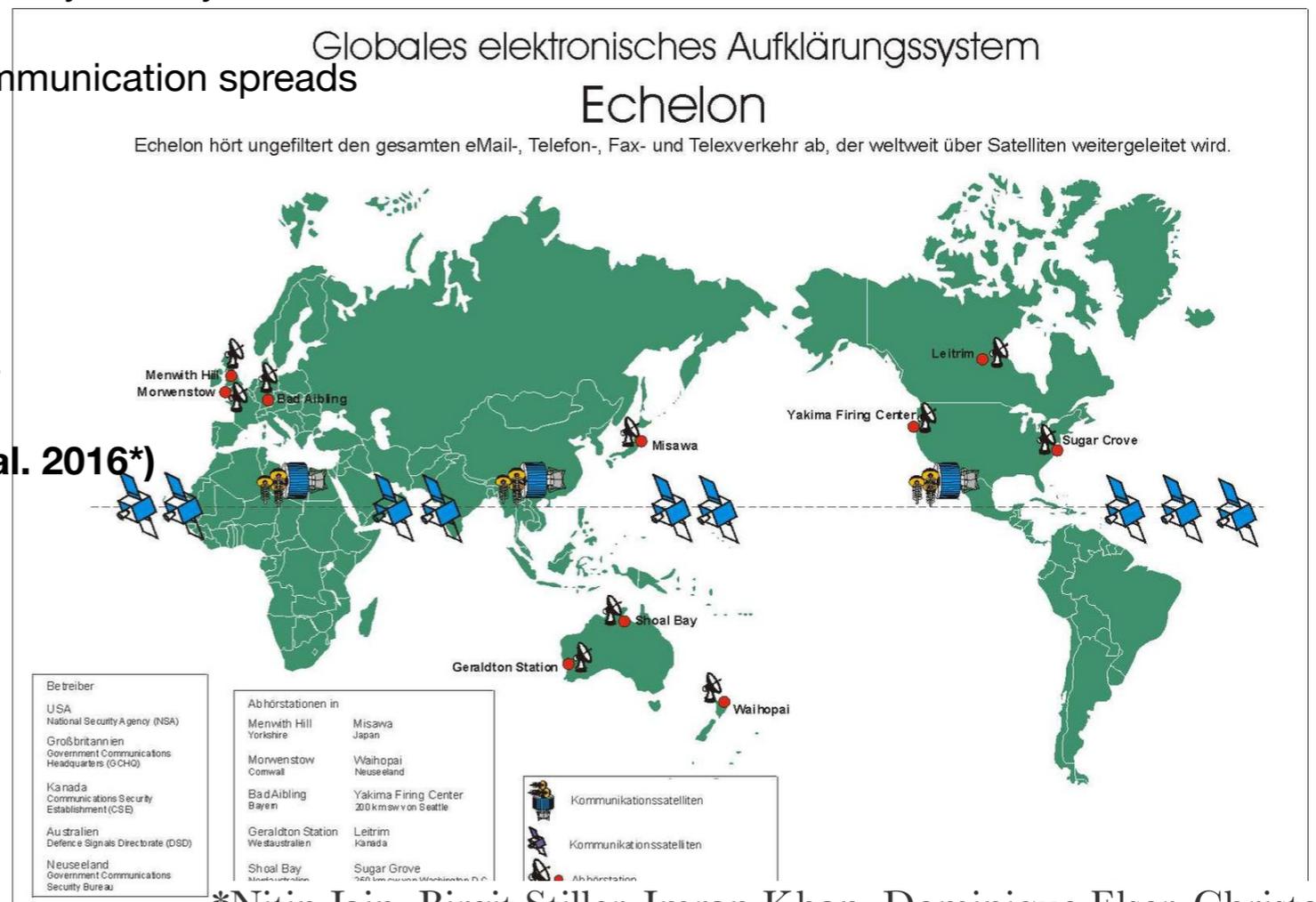
“Crypto-apocalypse”

But QKD not unbreakable - In some networks nodes' vulnerability)?

What does that mean in security terms?

1. All **SINGINT** (NSA, GCHQ, etc.) become blind, partially or totally: “going dark” (within approx 5 years - US quantum scientist - Kania & Costello, CNAS, 2018), actually already started?

- “Old” capabilities useless as quantum communication spreads
- SIGINT must develop new ways
- INT must use other ways
- Need for scientists to overcome blindness
- **Birth of Quantum Hacking (e.g. Jain et al. 2016*)**
- BUT talents shortage
- Race because the longer the blindness and the wider the blind spot, the more dangerous it becomes
- Changes in influence



*Nitin Jain, Birgit Stiller, Imran Khan, Dominique Elser, Christoph Marquardt & Gerd Leuchs (2016) Attacks on practical quantum key distribution systems (and how to prevent them), Contemporary Physics 57:3-2020-2027, DOI: 10.1080/10236198.2016.1141020

Countering Quantum Computing “Crypto-apocalypse”

2. Domestic security changes

- When quantum networks will be available at residential level
- Will organised crime and criminality benefit from quantum comm.?
- Need to revise all cyber police and cyber security (investments training, strategy, operations)
 - Can we break the security we created?
 - Need for talents
 - What happens until cyber police becomes operational again?



Source: Gendarmerie
Nationale -
Cybercriminalité

Countering Quantum Computing “Crypto-apocalypse”

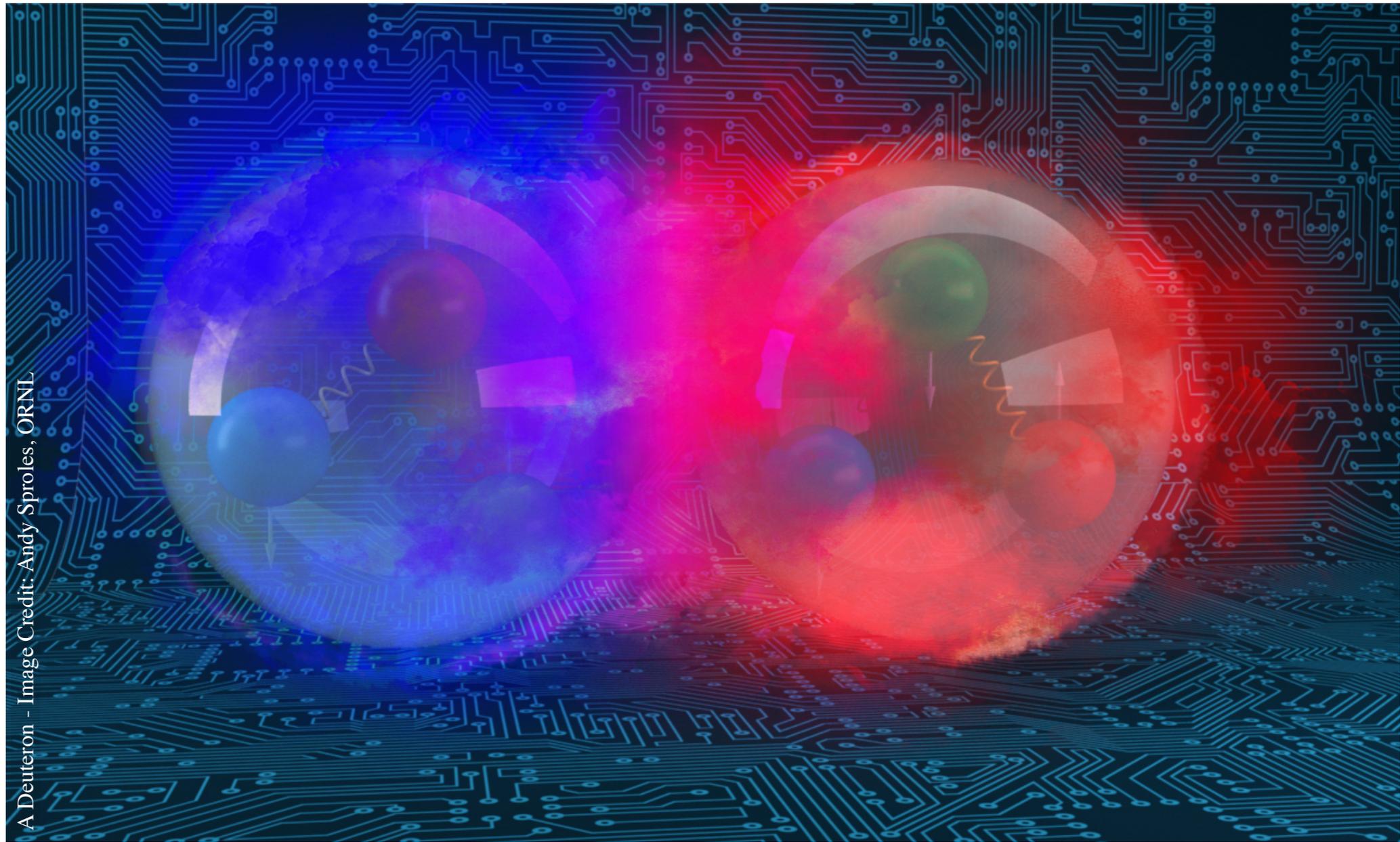
3. Security changes: economic and business

- Cybersecurity industry
 - Estimated market size between approx \$ 170 Billion by 2022 (Market Research Engine -“with data from 2015” [!!!!!!]) and \$248.26 Billion by 2023 (Markets and Markets)
 - Are you sure? Could the industry and its size be questioned?
- Companies providing communication infrastructures
- Companies using comm. infrastructures
- Quantum computing threatens blockchain*
- Adapted “cloud” actors?
- Others?

* Aleksey K. Fedorov, Evgeniy O. Kiktenko & Alexander I. Lvovsky, “Quantum computers put blockchain security at risk”, *Nature*, 19 November 2018

4. All levels: Could new Quantum Network Providers introduce “device” allowing them to “spy” on information exchanges?

- How do we know?
- How do we check?
- How to create trust?

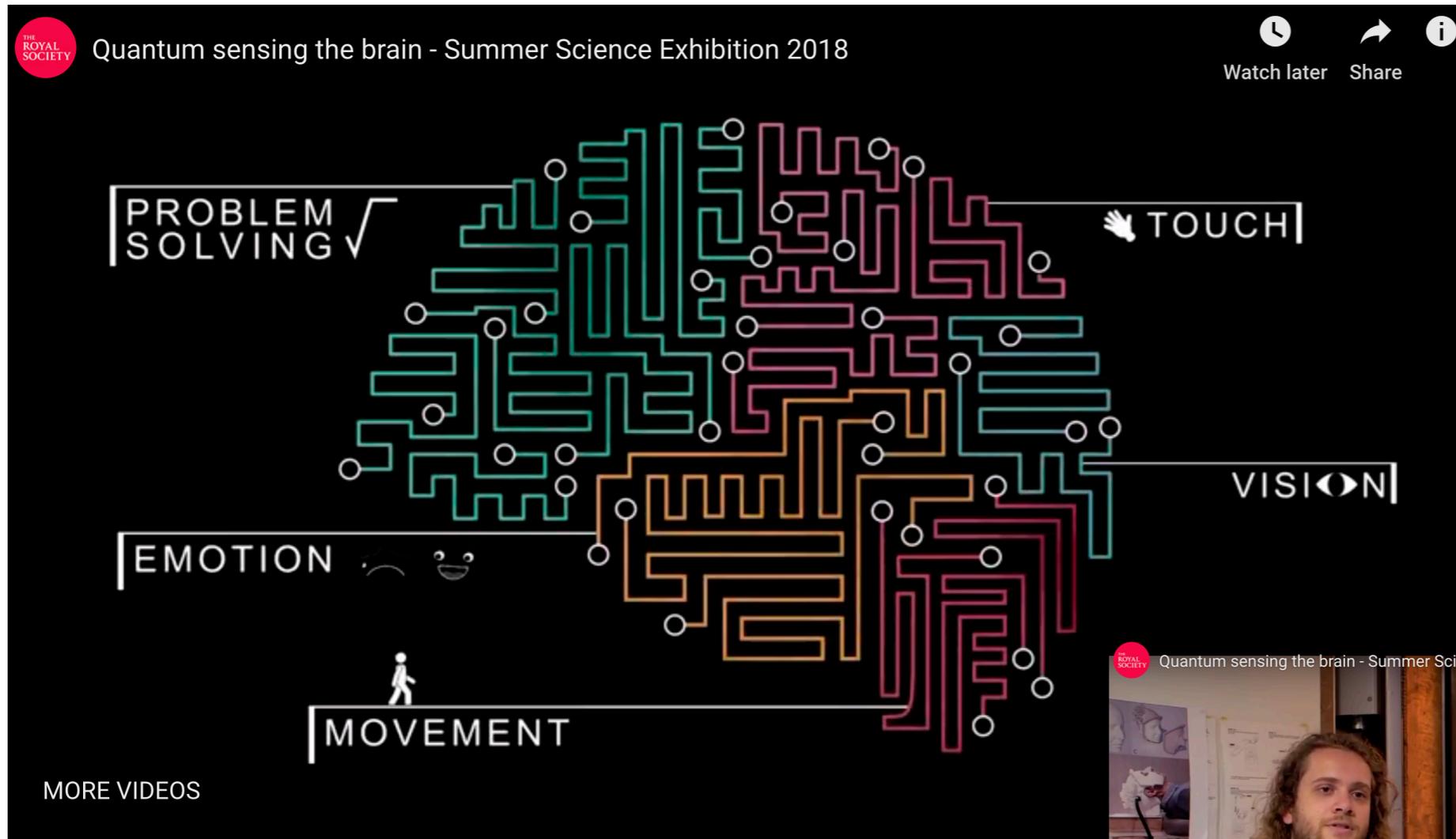


A Deuteron - Image Credit: Andy Sproles, ORNL

Quantum Sensing and Metrology

Quantum Sensing the Brain

University of Birmingham



Screenshots from the video - 11 June 2018 - for The Royal Society



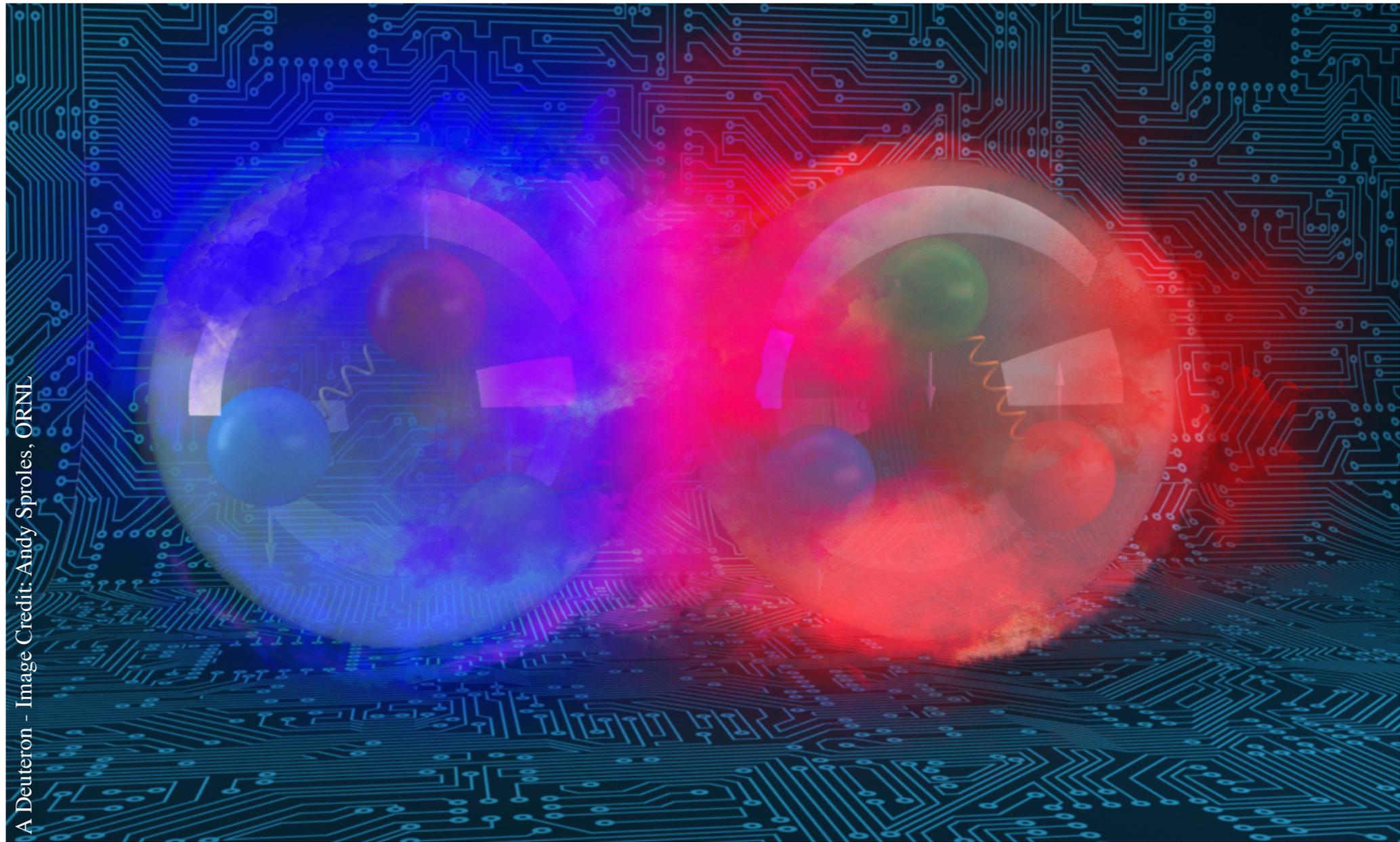
Could this new understanding impact AI and quest for a third generation AI (2bn USD investment by DARPA)... or even General AI? In turn, impact?

Changing the battlefield

- Notably radar, lidar, incl. for submarines communication
- But also quantum illumination defeating very new advances in meta materials e.g. cloaking (stealth technologies) (U. Las Heras et al., “Quantum illumination reveals phase-shift inducing cloaking”, *Scientific reports*, 24 Aug. 2017)
- Thus
 - Disrupted investments
 - Enhanced potential for surprise



Graphic by U.S. Army Acquisition Support Center and the authors) *Army AL&T*, October-December 2018 [Public Domain]



A Deuteron - Image Credit: Andy Sproles, ORNL

Quantum computing and simulations

From logistics and optimization to quantum smart ports
through solution to climate change

Logistics and optimization

VOLKSWAGEN
AKTIENGESELLSCHAFT



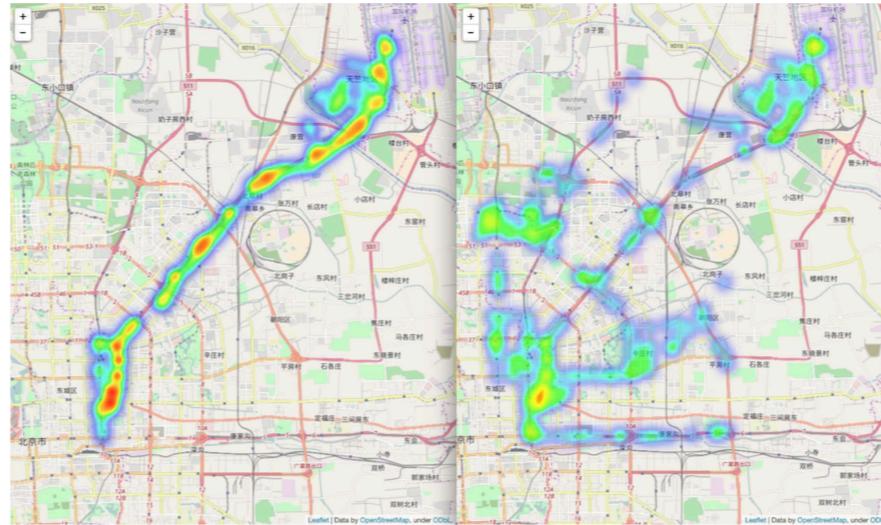
Quantum Computing at Volkswagen:
Traffic Flow Optimization using the D-Wave Quantum Annealer

D-Wave Users Group Meeting - National Harbour, MD
27.09.2017 – Dr. Gabriele Compostella

VOLKSWAGEN
AKTIENGESELLSCHAFT

Result: unoptimised vs optimised traffic

DATA:LAB
MUNICH



27.09.2017

K-S/ILD | Dr. Gabriele Compostella

18

Microsoft and DEWA bringing quantum computing to Dubai
June 28, 2018 | Microsoft News Center



Smart cities worldwide



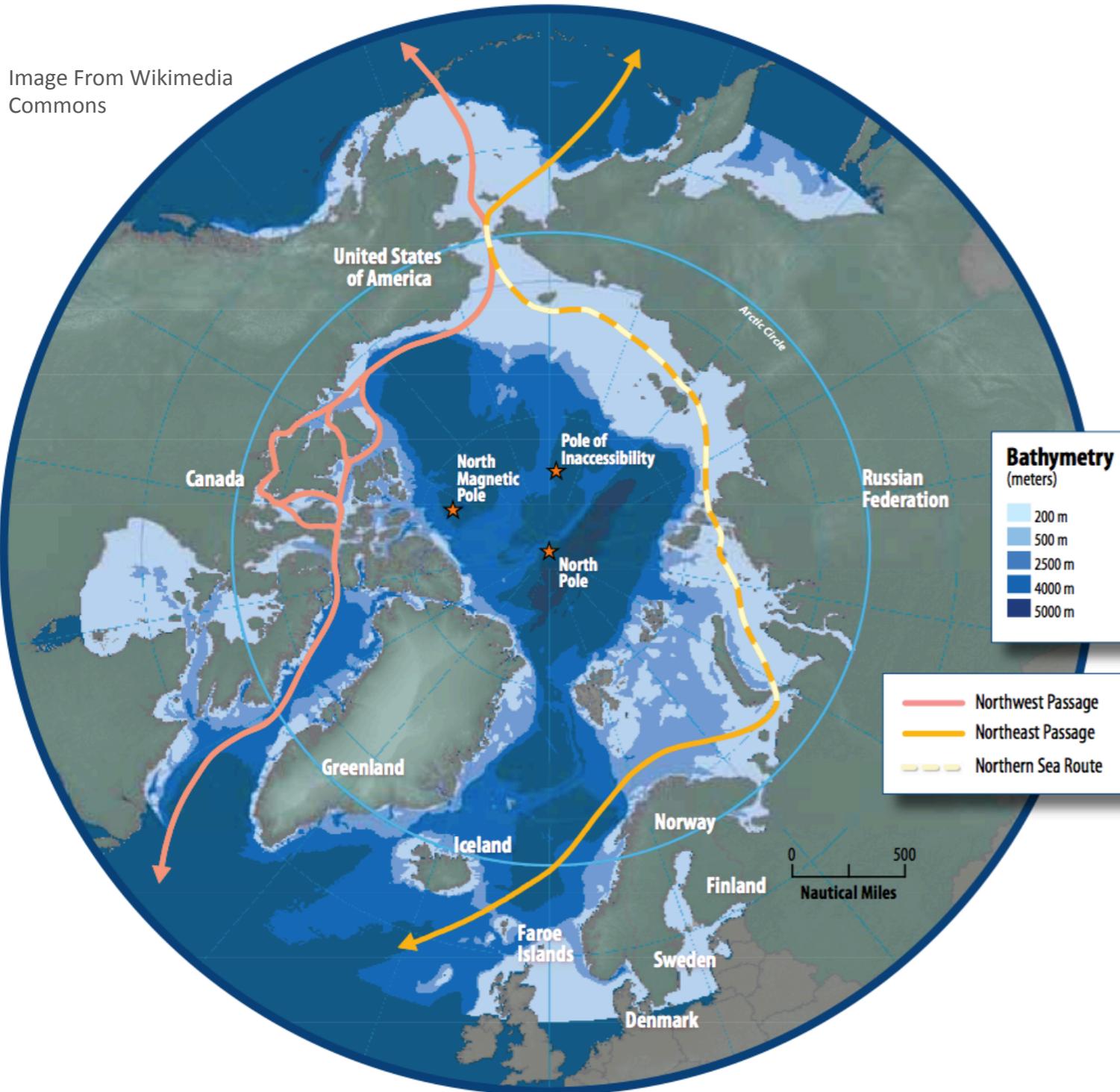
A modern Army needs modern installations
By Dr. Jason R. Dorvee, U.S. Army
September 17, 2018



The guided-missile destroyer USS Mustin (DDG 89) receives cargo from the Military Sealift Command fleet replenishment oiler USNS Tippecanoe (T-AO 199) -U.S. Navy photo by Mass Communication Specialist 2nd Class Devon Dow/Released [public domain]

The Northern Sea Route and Quantum Smart Ports

Image From Wikimedia Commons



Shanghai Zhenhua Heavy Industry Image Map

Source: Shanghai Zhenhua Heavy Industry 2018/4/10 11:17:08

Screenshot from Shanghai Zhenhua Heavy Industry Website

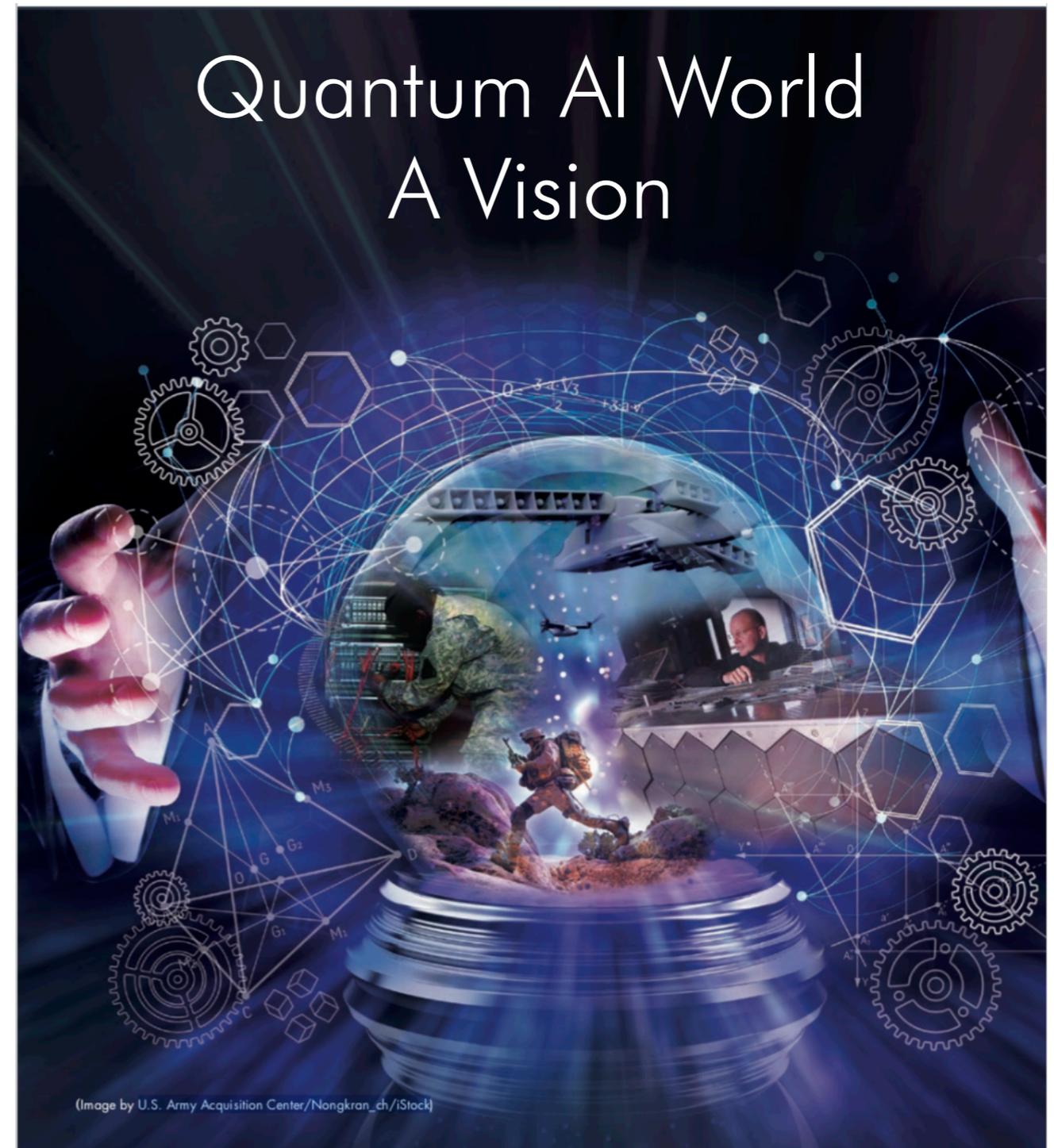


APEC Economic Leaders' Meeting in Danang. November 10, 2017

+ Project of trans-Arctic fiber-optic data cable that would connect Finland, Norway and Russia with Japan and China... with QKD?

Key - Building an Adapted Strategic Foresight Process

- Because imagining and allowing imagining the Quantum AI world (with evidence) is crucial, **notably for stakeholders**
- Quantum Computing actors should include an adapted SF process
 - Dynamic and evolving with latest scientific and engineering findings
 - Multidisciplinary
 - Considers 'security' for all actors
 - Delivers the imagined world in the best possible format (according to audience)



2

The Race for Quantum

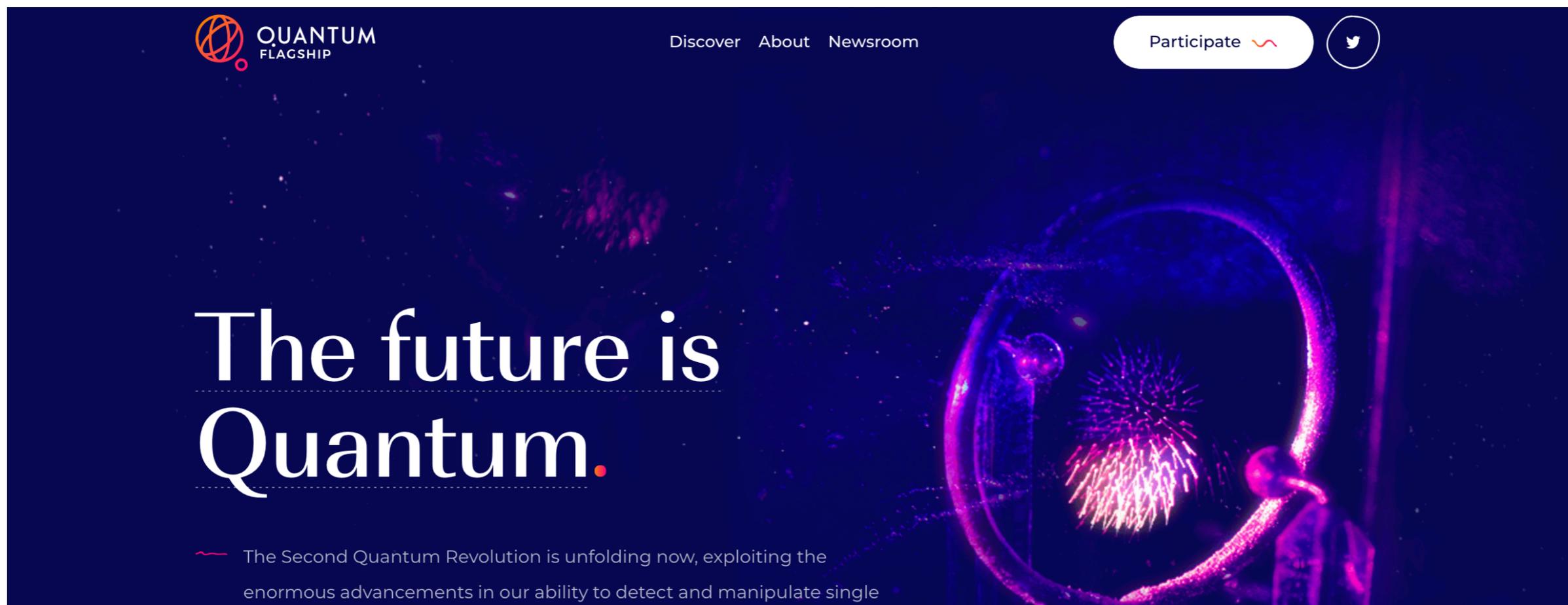


Characteristics of a race

- Looking only at overall state funding (as in the race to exascale HPC) is at best unsatisfactory
- The ongoing quantum race is complex
- From “The state of the race” to “how can we understand it best?”

Characteristics of a race

- Public comprehensive strategic framework (or not)
- Yearly usual public research funding
- Public-private Industry-Research... and Finance (pre-seed venture capital?)
- Across sovereign boundaries with industrial risks and sovereign national security risks
- Onset of efforts (when did it start?) Time and accumulated funding, research, notoriety matter
- Funding matters, but talents too, how to capture the two (publications?)
- What about tomorrow talents?
- Communication matters too (capturing imagination), how to measure it?

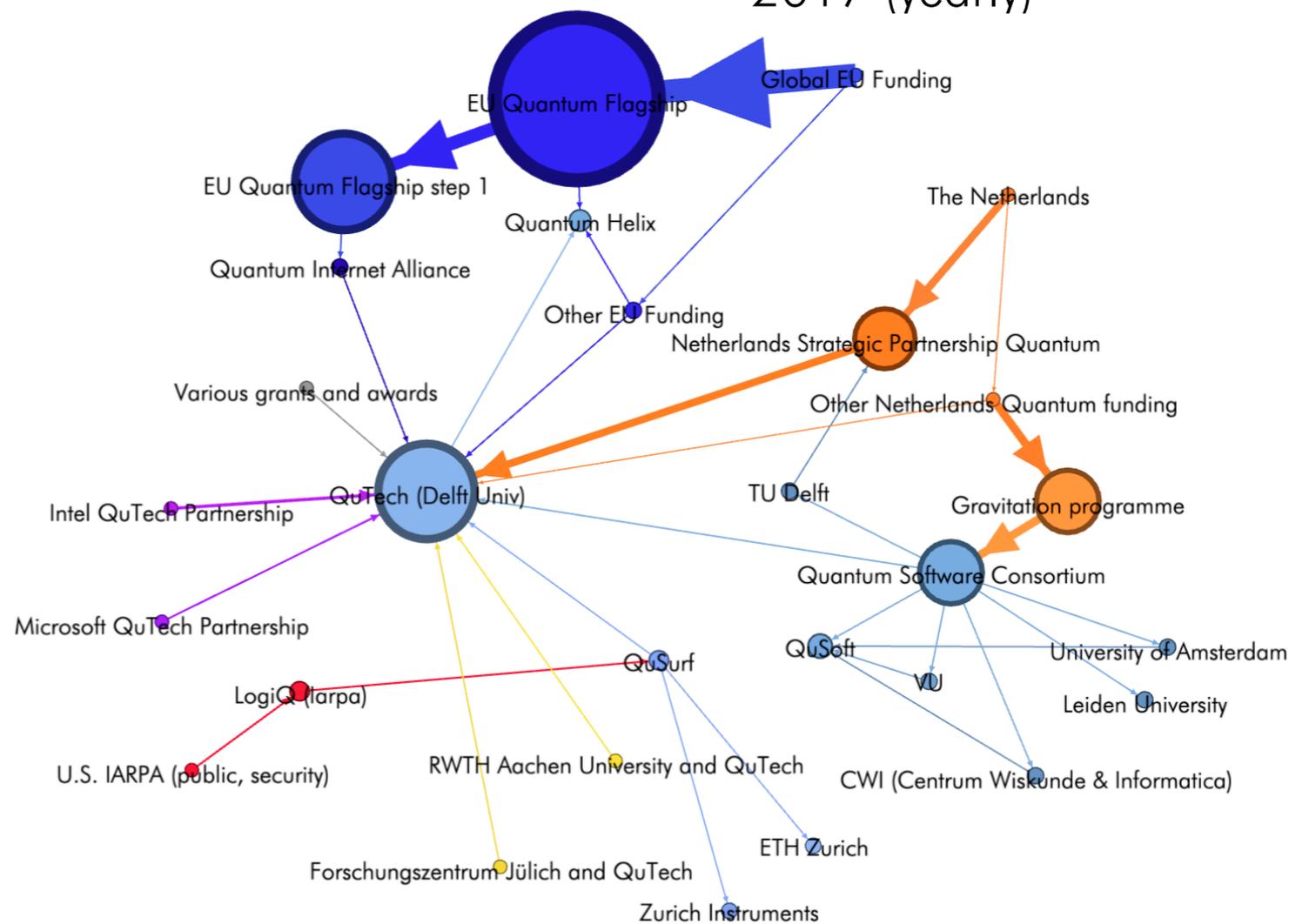


Mapping the Race to Quantum

The Netherlands and QuTech

- The Netherlands
“Comprehensive strategic framework”: €146 million over 10 years (\$168,6 million) received from the government (QuTech Annual Report 2015 p.7, 35)
- However QuTech also enters in various partnerships and alliances (QuTech Annual Report 2017).
 - Public Private: e.g. Intel and Microsoft.
 - Across Boundaries beyond EU: US IARPA.

Mapping the Race to Quantum
Example - QuTech Funding 2017 (yearly)



Graph done with Gephi
Sources: QuTech Annual Report 2017

© H Lavoix - The Red (Team) Analysis Society

Mapping the Race to Quantum

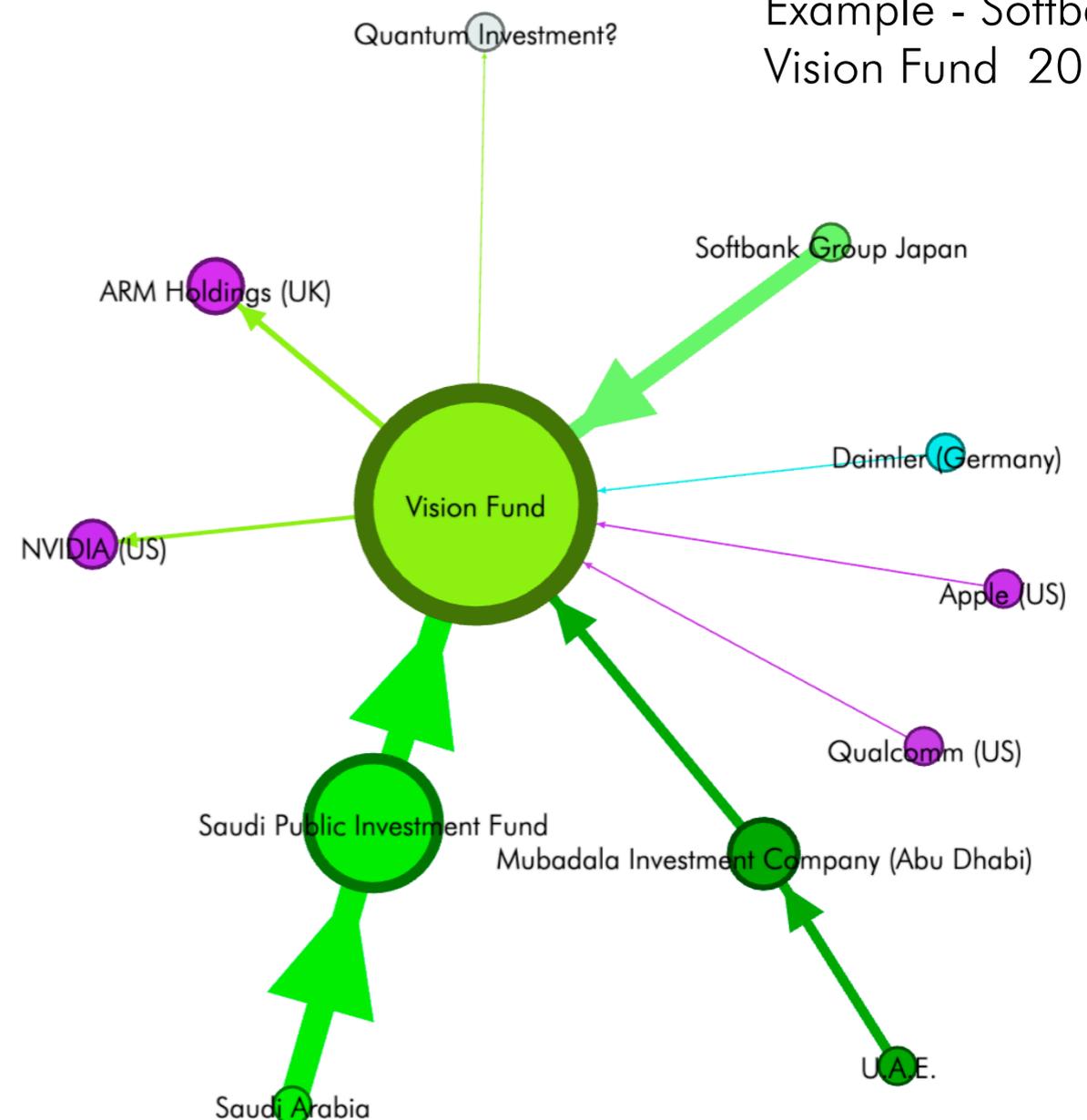
Softbank Vision Fund?

- 100 billion USD Fund - Minimum investment 100 million USD - Managed in London
- Want to find and back the company whose quantum computing hardware or software that runs atop it would become the “de facto industry standard”

“We are happy to invest enough to create that standard around which the whole [Quantum] industry can coalesce”.

Shu Nyatta, Vision Fund, reported by Jeremy Kahn, [“SoftBank's Vision Fund Eyes Investment in Quantum Computing,”](#) Bloomberg Quint, 26 June 2017.

Mapping the Race to Quantum
Example - Softbank Vision Fund 2018



Sources: Vision Fund website, FT, Bloomberg

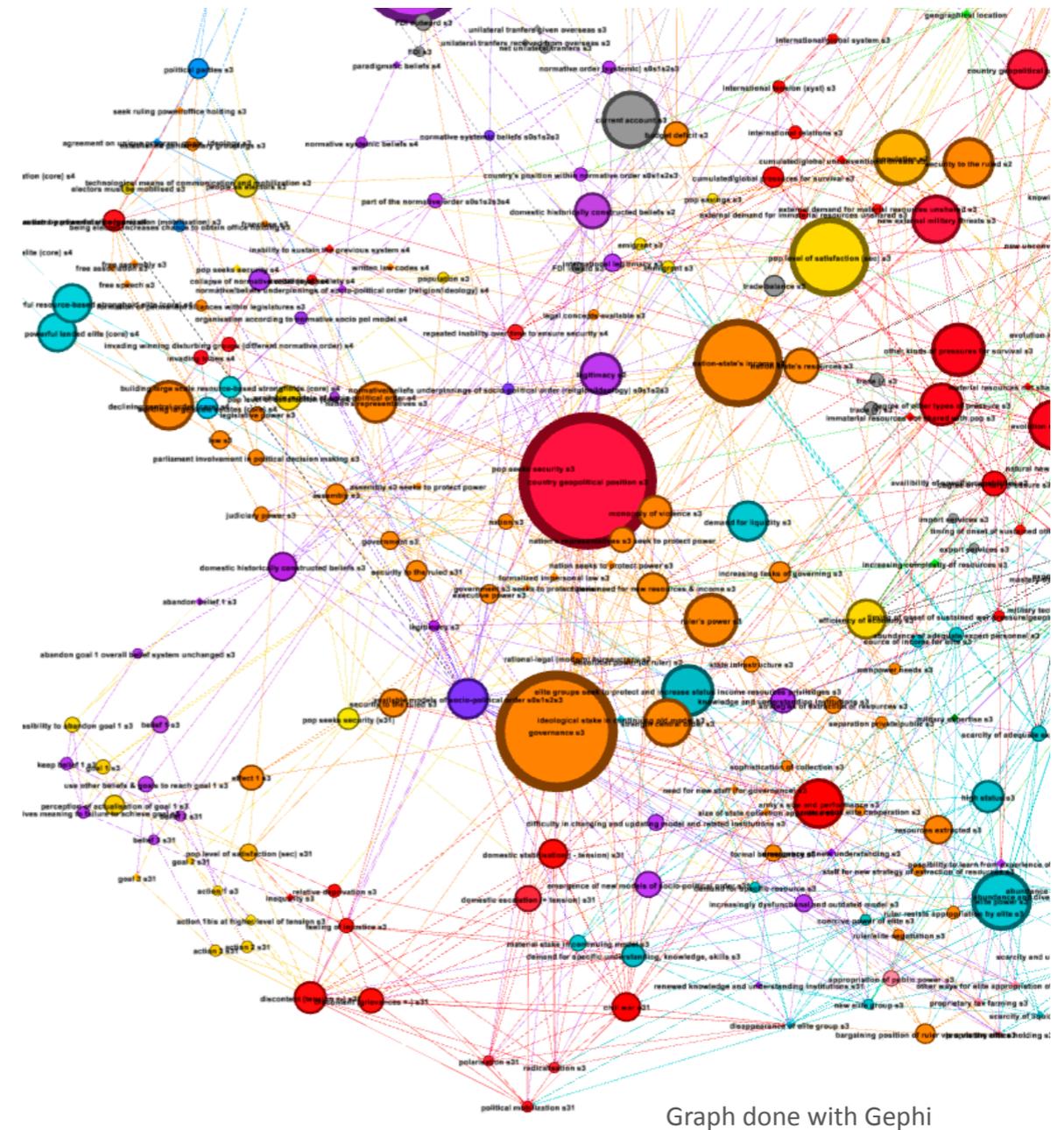
© H Lavoix - The Red (Team) Analysis Society

Graph done with Gephi

Key - Mapping the Quantum Race

Research in progress -

- The complete Quantum Race should be mapped.
- Dynamic mapping: [video see article on RTAS](#)
- Translation Global investment/ Yearly budget.
- The other characteristics of the race, as much as possible, should be included.



Further references - China

“It is planned to invest 100 billion yuan in five years (\$14.39 billion over 5 years, i.e. \$2.878 billion per year) for the National Laboratory of Quantum Information In Hefei”

Pan Jianwei Introduction. Reporter Zhang Pei

“CAS Academician is a guest at the Hefei Municipal Committee Central Group Theory Study Conference on Quantum Communication” [中科院院士做客合肥市委中心组理论学习会讲量子通信], Anhui Business Daily, May 24, 2017 http://ah.ifeng.com/a/20170524/5694552_0.shtml

Kania, Elsa B. & John K. Costello, QUANTUM HEGEMONY? China's Ambitions and the Challenge to U.S. Innovation Leadership, CNAS, September 2018.

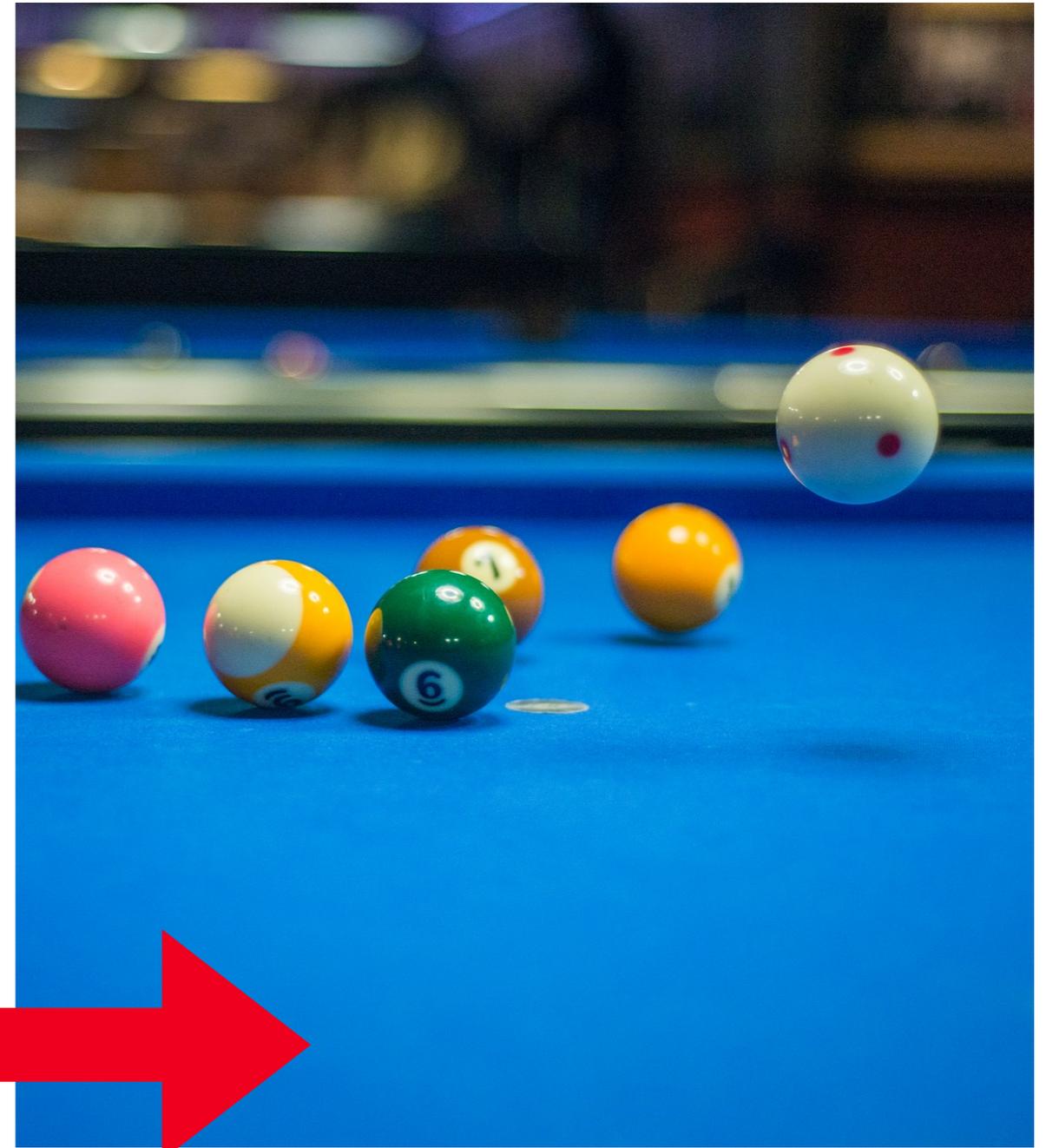
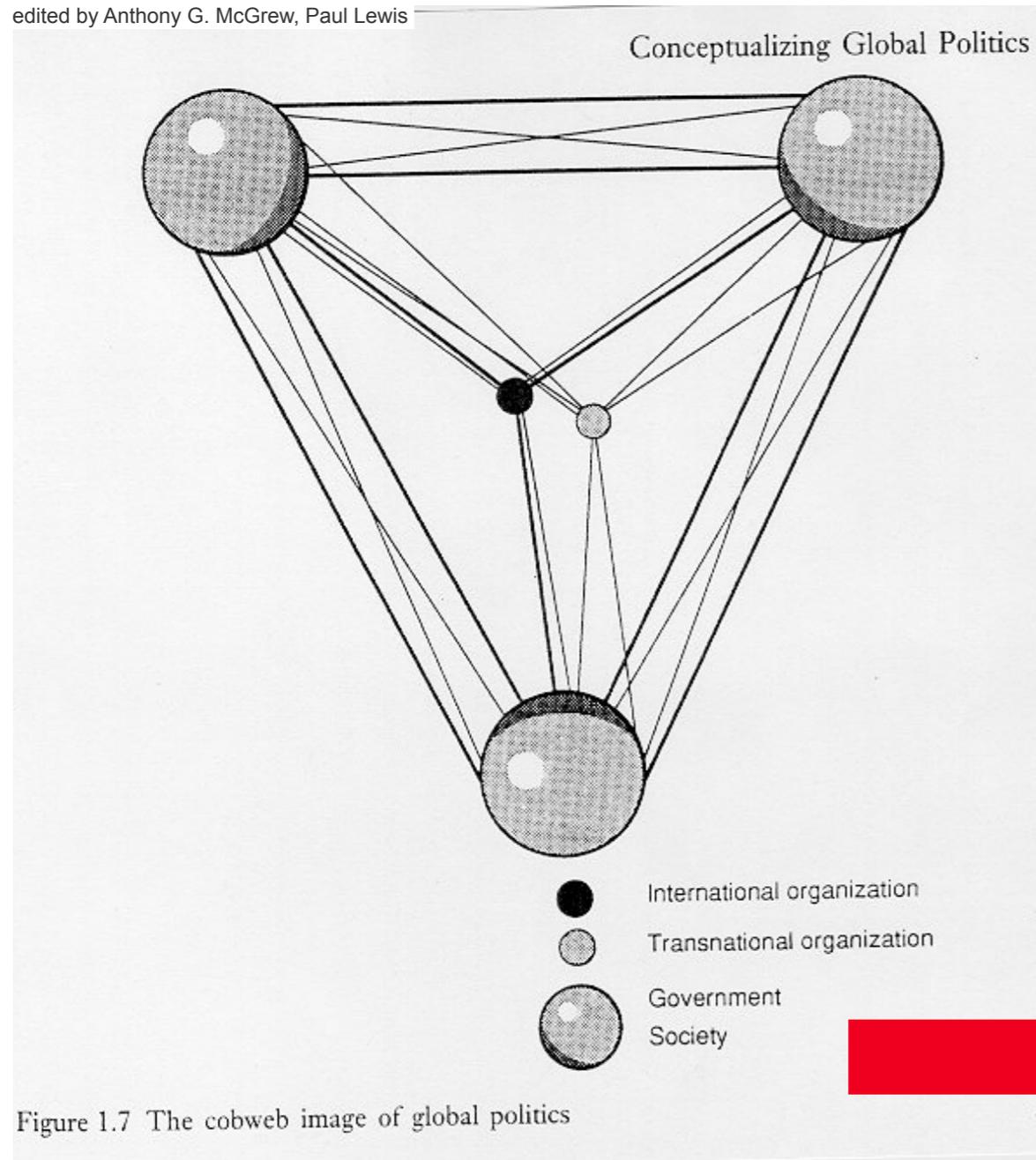
3 What if.....



Two main paradigms to see the world

Source: *Global Politics: Globalization and the Nation-State*

edited by Anthony G. McGrew, Paul Lewis



The Quantum Race Now?

The Quantum Race Tomorrow?

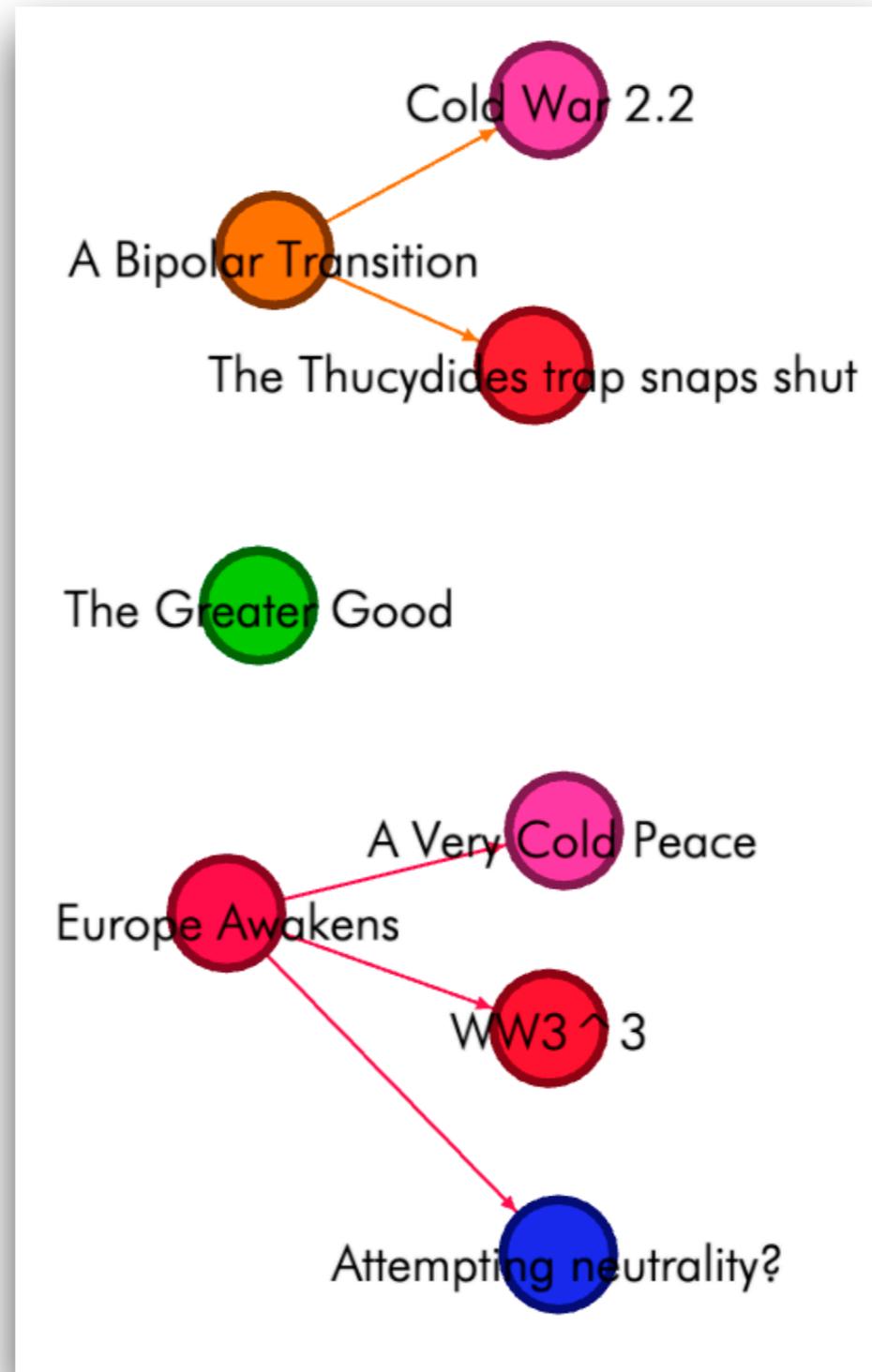
Selected Signals that we are changing IR paradigm

Towards a more “security-sensitive”, national interest-led world

- Climate change
- An international system in transition, highly polarised, moving from a unipolar world dominated by the U.S. to ?:
 - Unipolarity - U.S. or China
 - Bipolarity: U.S. + allies vs China- Russia + sphere of influence
 - Tripolarity: + European states

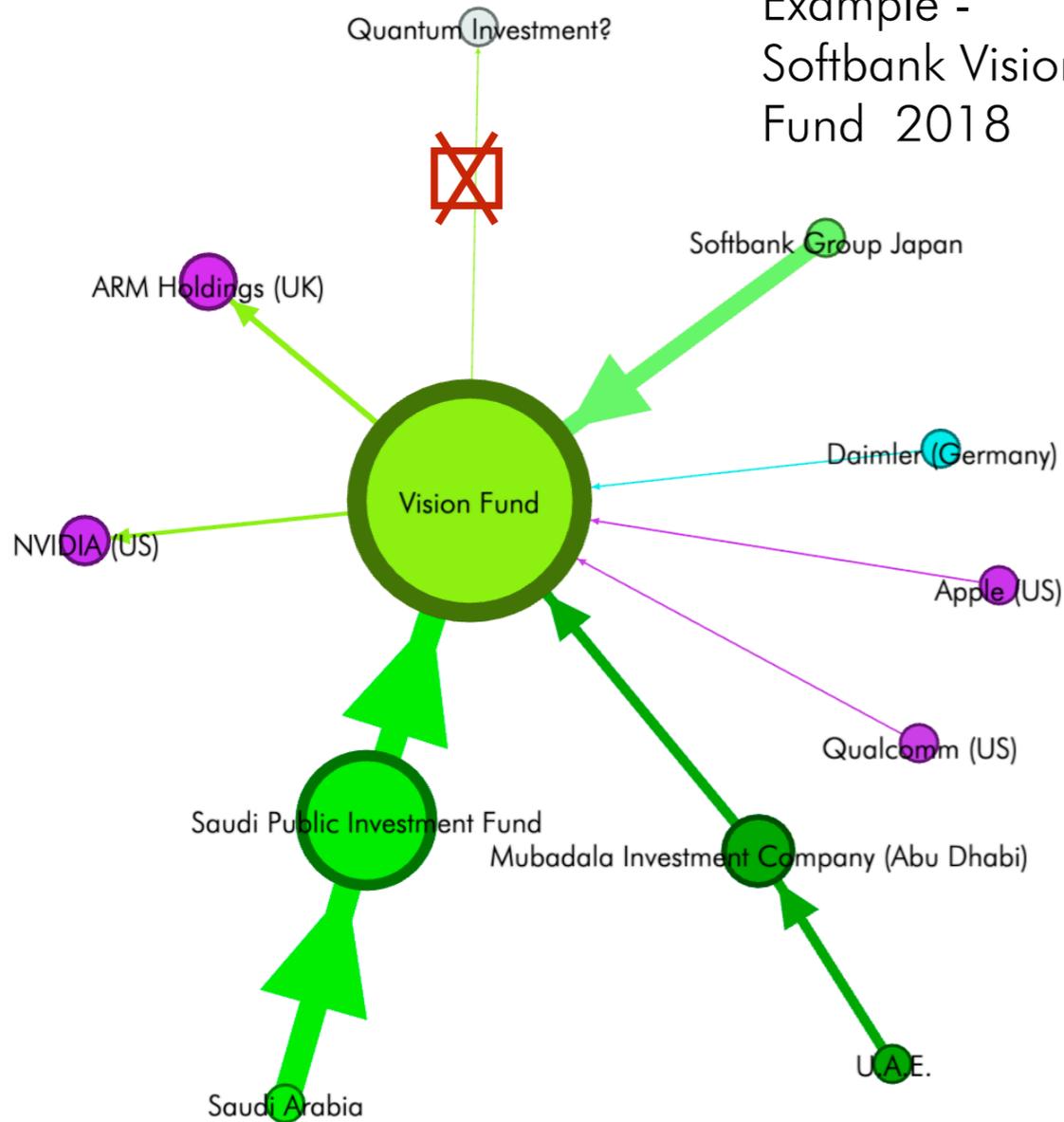
The screenshot shows the Federal Register website interface. At the top, there is a navigation bar with options like 'Sections', 'Browse', 'Search', 'Reader Aids', and 'My FR'. Below this is the 'FEDERAL REGISTER' logo and the text 'The Daily Journal of the United States Government'. A blue banner highlights a 'Proposed Rule'. The main content area features the title 'Review of Controls for Certain Emerging Technologies' and a sub-header 'A Proposed Rule by the Industry and Security Bureau on 11/19/2018'. A green button labeled 'SUBMIT A FORMAL COMMENT' is visible. On the right, a 'DOCUMENT DETAILS' sidebar lists: 'Printed version: PDF', 'Publication Date: 11/19/2018', 'Agencies: Bureau of Industry and Security', and 'Dates:'. A red arrow points from the '11/19/2018' date to a large blue box at the bottom of the page that contains the text '19 November 2018' in red.

Key - A possible set of scenarios

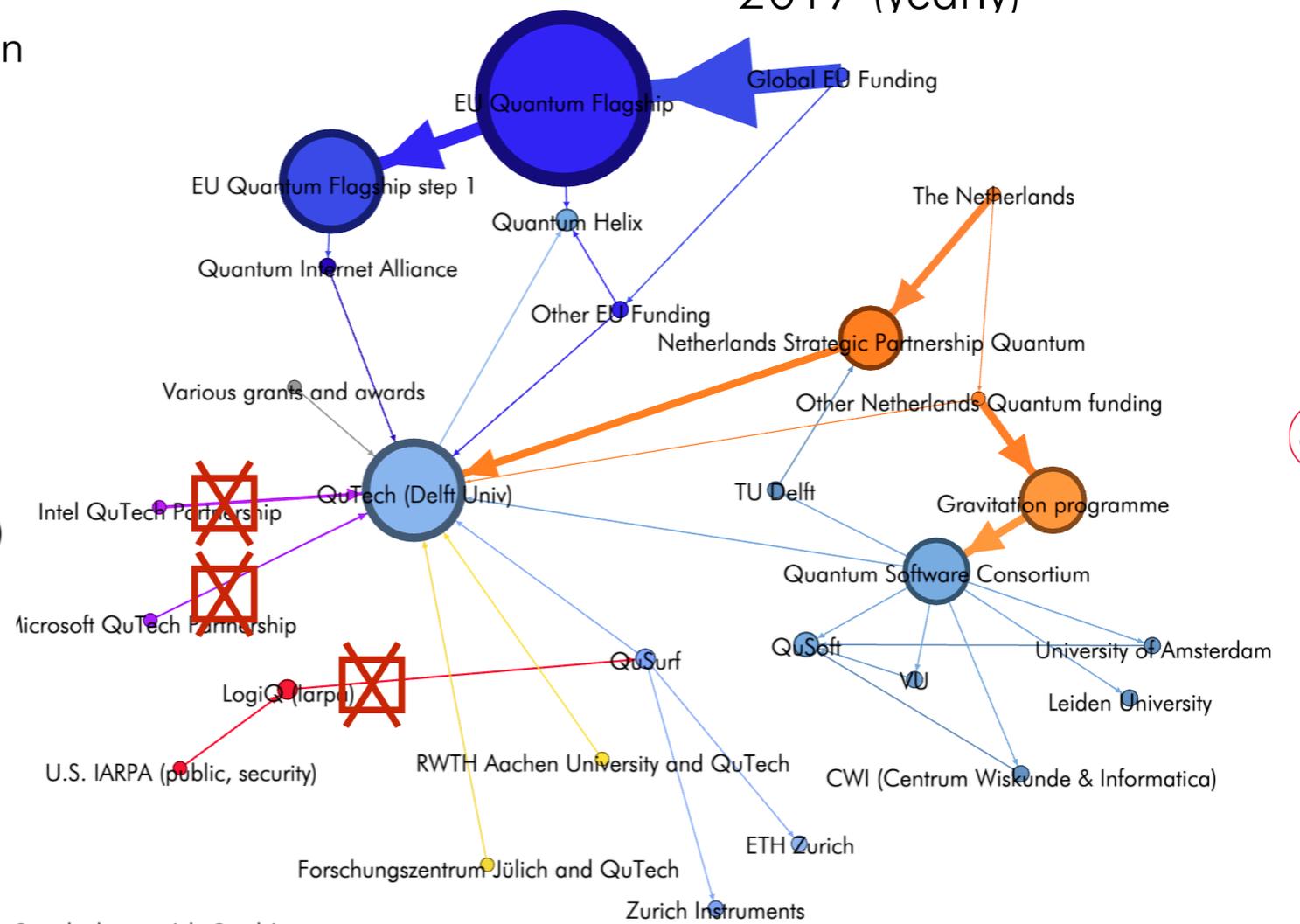


Key - Applying Scenarios

Mapping the Race to Quantum
Example - Softbank Vision Fund 2018



Mapping the Race to Quantum
Example - QuTech Funding 2017 (yearly)



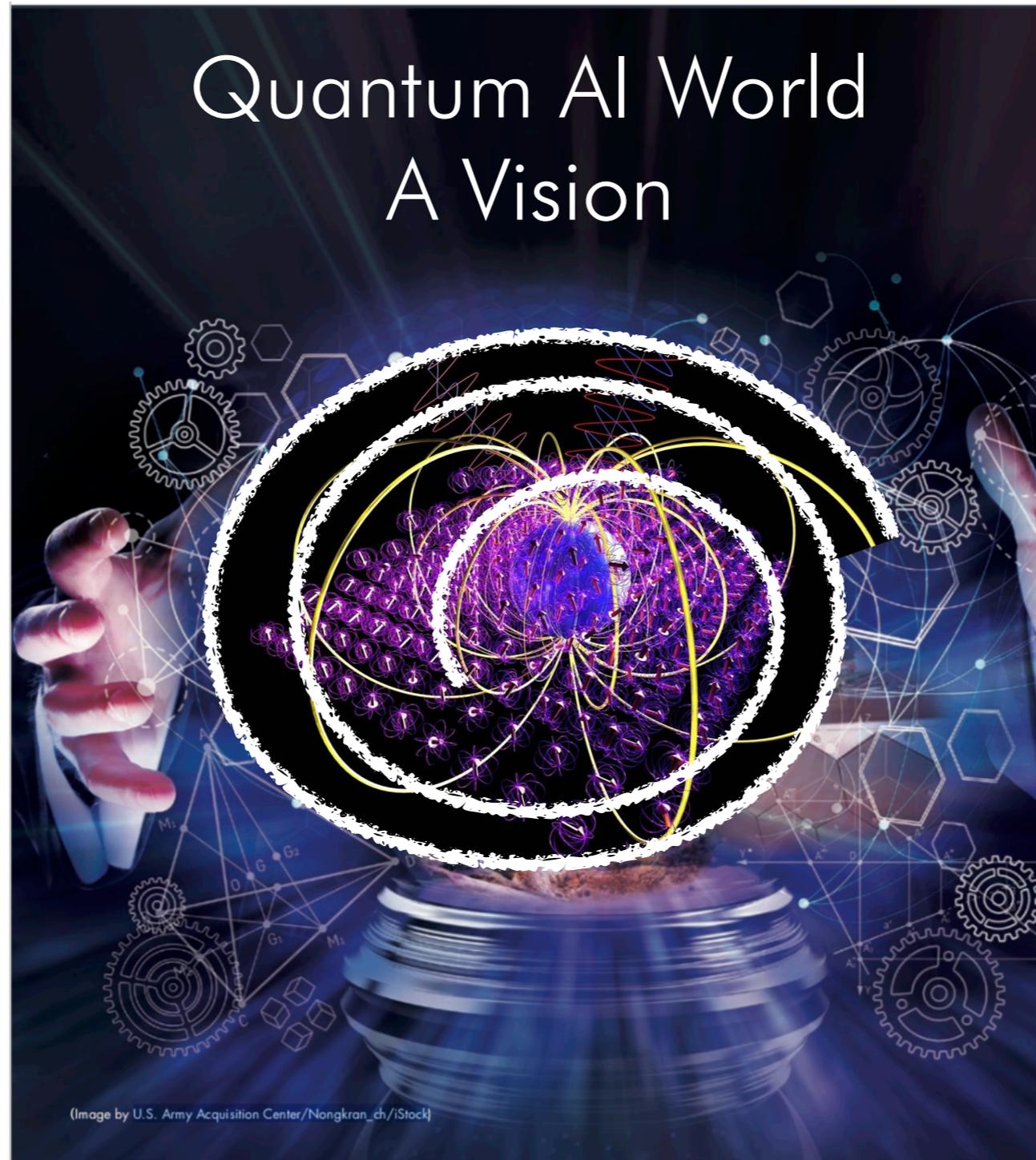
Graph done with Gephi
Sources: QuTech Annual Report 2017

© H Lavoix - The Red (Team) Analysis Society

© H Lavoix - The Red (Team) Analysis Society

Graphs done with Gephi

Key - Applying Scenarios



Graphs done with Gephi

About the Speaker



Dr Helene Lavoix (MFin Paris, MSc PhD Lond)
Director, The Red (Team) Analysis Society;
Lecturer, Member of the Faculty at SciencesPo-PSIA;
Member of Agora 41 (ANSSI).

She is the founder of The Red (Team) Analysis Society and a political scientist (International Relations) specialised in Strategic Foresight and Warning (SF&W) for conventional and unconventional security issues. She teaches Strategic Foresight and Warning, both in universities, at Master level (e.g. since Autumn 2015 (4 years) at Sciences-Po-PSIA in Paris, France, 2011 & 2010 RSIS Singapore), and in executive courses (e.g. 2017-2013 Vesalius College Brussels, 2015 Geneva Centre for Security Policy). She has notably been the coordinator of the Strategic Foresight and Warning Community of Interest of the GFF (2013-2007), an independent consultant on SF&W, an analyst for the European Commission, the head of the Cambodian office of an NGO, and prior to that, worked in finance, as a treasurer.

Besides writing extensively for The Red (Team) Analysis Society, she is the author of “Ensuring a Closer Fit: Insights on making foresight relevant to policymaking”, *Development* (2014) 56(4); “What makes foresight actionable: the cases of Singapore and Finland” (confidential commissioned report, US government, November 2010), “Enabling Security for the 21st Century: Intelligence & Strategic Foresight and Warning” RSIS Working Paper August 2010, “Constructing an Early Warning System,” in *From Early Warning to Early Action*, European Commission, ed. DG Relex, 2008, “Detailed chronology of mass violence – Cambodia (1945 – 1979),” *Online Encyclopaedia of mass violence*, 2008 and the editor of *Strategic Foresight and Warning: Navigating the Unknown*, ed. RSIS-CENS, February 2011; etc.

helenelavoix@redanalysis.org

www.redanalysis.org



Thank You!

Q&A

helenelavoix@redanalysis.org
www.redanalysis.org

