Potential Implications of Quantum Science and Technology for Global Security

ELSA B. KANIA

ADJUNCT SENIOR FELLOW, TECHNOLOGY AND NATIONAL SECURITY

“If it is correct, it signifies the end of science.”

—Albert Einstein

“*Those who are not shocked when they first come across quantum theory cannot possibly have understood it.*”

—Niels Bohr

“Any sufficiently advanced technology is indistinguishable from magic.”

— Arthur C. Clarke

Initial Caveats

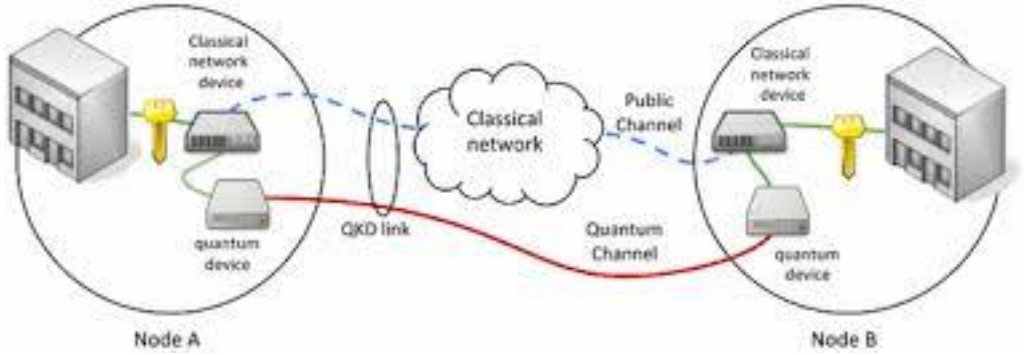
- uncertainties of timeframes and trajectories of quantum science and technology
- potential for technological surprise or unexpected strategic latency
- level of hype and exaggerated expectations
- limited availability of information and questions of veracity
- necessarily, only initial, rather speculative conclusions

Overview of Assessments

- The employment of quantum cryptography contribute to improved security (i.e., it's 'uncrackable'), but hardly provides a perfect solution.
- At present, quantum computing, which could enable massive increases in computing capabilities, remains a more distant possibility, despite robust progress and massive investments.
  - However, the potential of quantum computing to crack prevalent cryptography is a threat that requires near-term adjustment to the use of post-quantum encryption.
- The initial advances in quantum networking – and notion of a future quantum internet – is intriguing but remains nascent.
- In the near term, quantum technologies also have promising applications in defense.
  - The use of quantum navigation can provide a more resilient alternative to GPS.
  - The potential of quantum radar and sensing has more direct military relevance.

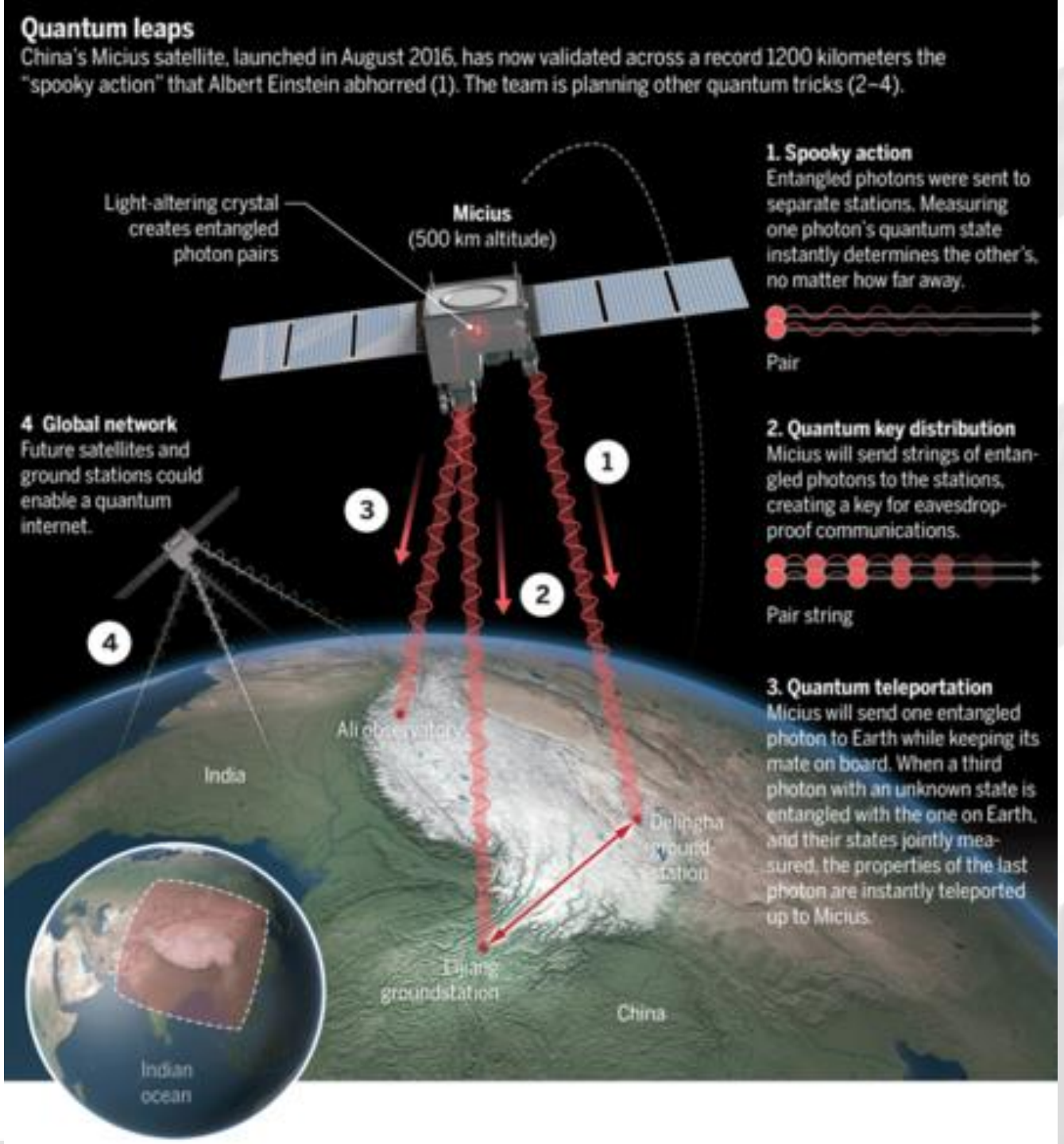
Quantum Cryptography

- primarily involving Quantum Key Distribution (QKD)
  - secure exchange of cryptographic key through entanglement
- implemented over optical fiber or with key exchange via satellite to enable at scale
- “absolute security” or perhaps marginal benefits
- risks of interference and potential vulnerability to ‘hacking’ or spoofing, despite progress
  - e.g., side-channel attacks



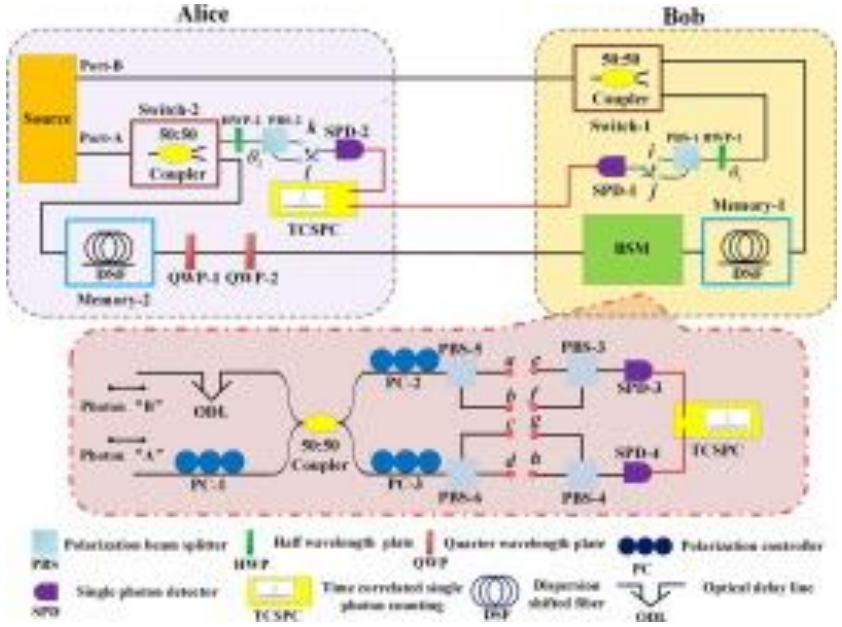
Quantum Satellites

- use of satellites to enable quantum communications (e.g., via QKD) at greater distance
- launch of Micius in Aug. 2017 as proof of concept
- plans to expand into entire constellation
  - potential applications in military communications



Quantum Communications

- particularly secure direct communication in which information itself transmitted through entanglement
- option for fiber, free air, or underwater transmission
  - potential communication with submarines
- potential evolution towards quantum networking to enable quantum internet designed for security



China's National Quantum Communications Infrastructure

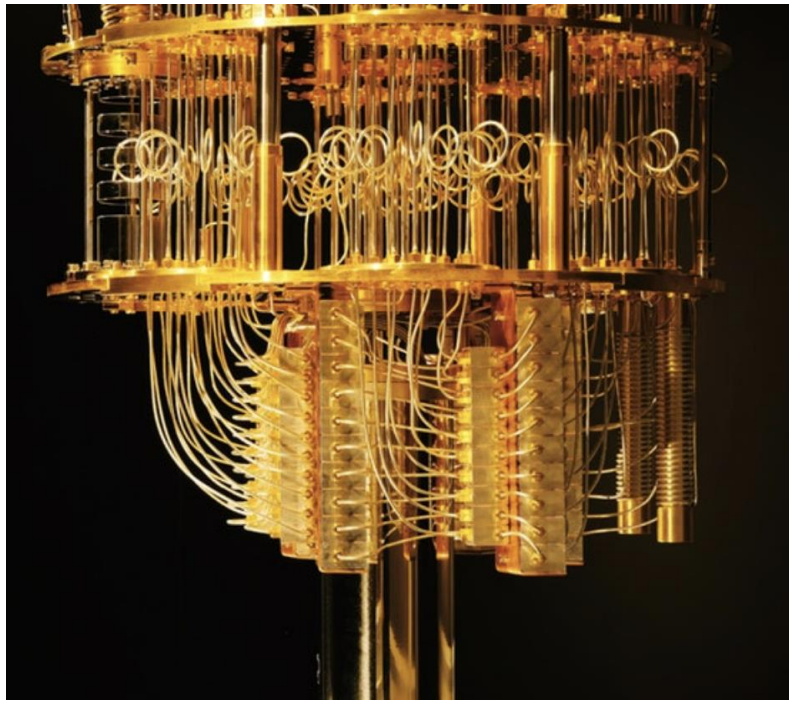
- expansion of national quantum communications infrastructure leveraging quantum key distribution (QKD) over local and backbone networks
  - new line linking Hefei and Wuhan connected to initial Beijing-Shanghai trunk, in conjunction with local networks
  - adoption and connection by local industry and governments, including major banks, military units, etc.

Potential for Future Information and Intelligence Asymmetries?

- in anticipation of future realization of quantum computing, option of “wait and see” collection
- potential for emergence of information and intelligence asymmetries
- perhaps even destabilizing influence through undermining the efficacy of intelligence collection
- actual effect will depend upon implementation
- question of relative timeframes of emergence of quantum computing versus replacement of current encryption with alternatives of quantum-resistant encryption

The *Marathon* for Quantum Computing

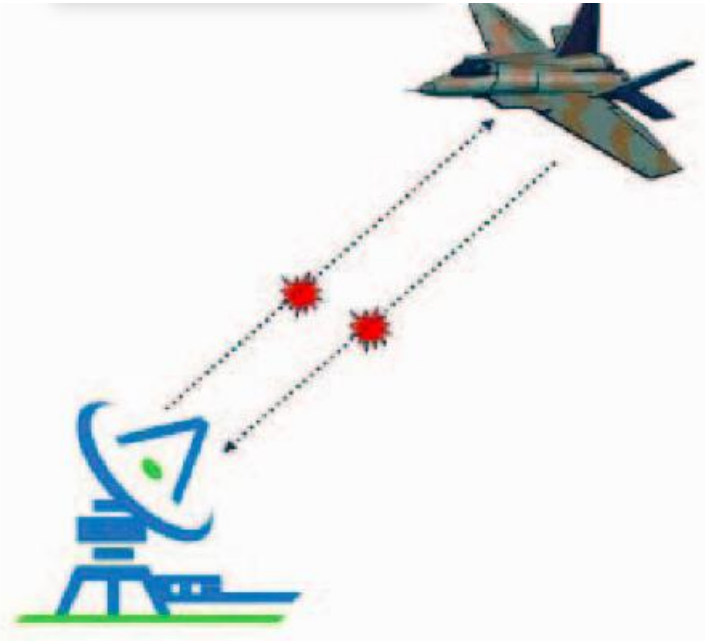
- progress along parallel pathways, including photonic qubits, superconducting qubits, etc.
  - advances in development of photon quantum computer (used for boson sampling), large-scale optical quantum chips, new quantum computer control system, etc.
    - ➢ China's record for entanglement among 18 qubits
- robust commercialization among leading international companies and growing number of start-ups
- goals extend beyond "quantum supremacy" by 2020, to objective of producing prototype and *eventually* functional quantum computer




密码破译
Code breaking
优化问题
Optimization problem
量子化学
Quantum chemistry

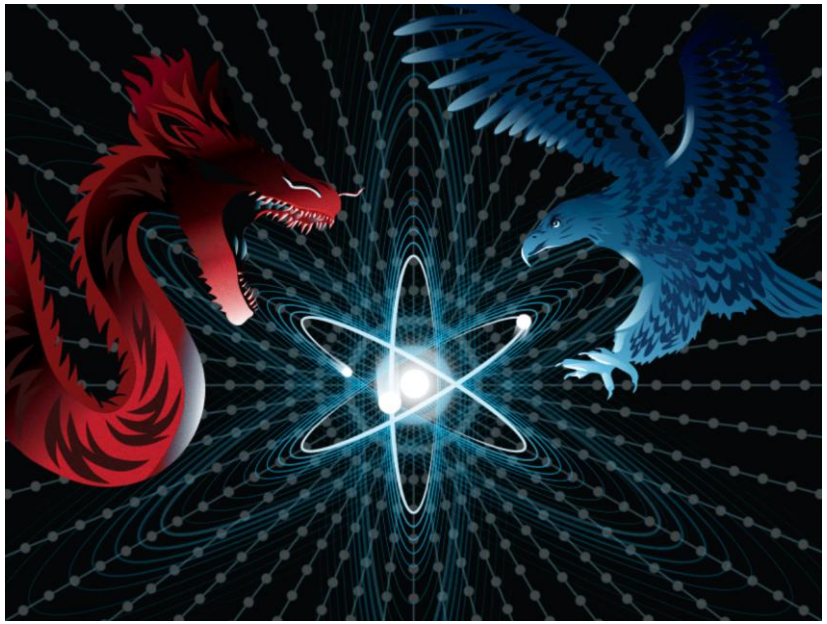
Quantum Radar and Sensing

- leveraging quantum properties for improved sensitivity and enhanced capabilities in detection
  - e.g., concept and demonstration of single photon quantum
- advances in quantum sensing, imaging, and magnetometry
- varying assessments of extent of disruption
  - how much better than best classical alternatives?
- active research for defense applications, but uncertainty about relative maturity



Geopolitics of Quantum Science and Technology

- openness in basic research, involving extensive international collaboration
- juxtaposed with intense competition (and growing secrecy?) among companies seeking commercial advantage, particularly in quantum computing
- massive investments and perhaps exaggerated expectations
  - e.g., quest for ‘quantum supremacy’ as primarily symbolic milestone
- launch of national initiatives in China, European Union, United States, along with promising research in Japan, Canada, Australia
- growth and expansion of field globally and potential shifting in patterns of collaboration



“Scientists are beginning to control the quantum world; this will greatly promote the development of information, energy, and materials sciences, bringing about a new industrial revolution.”

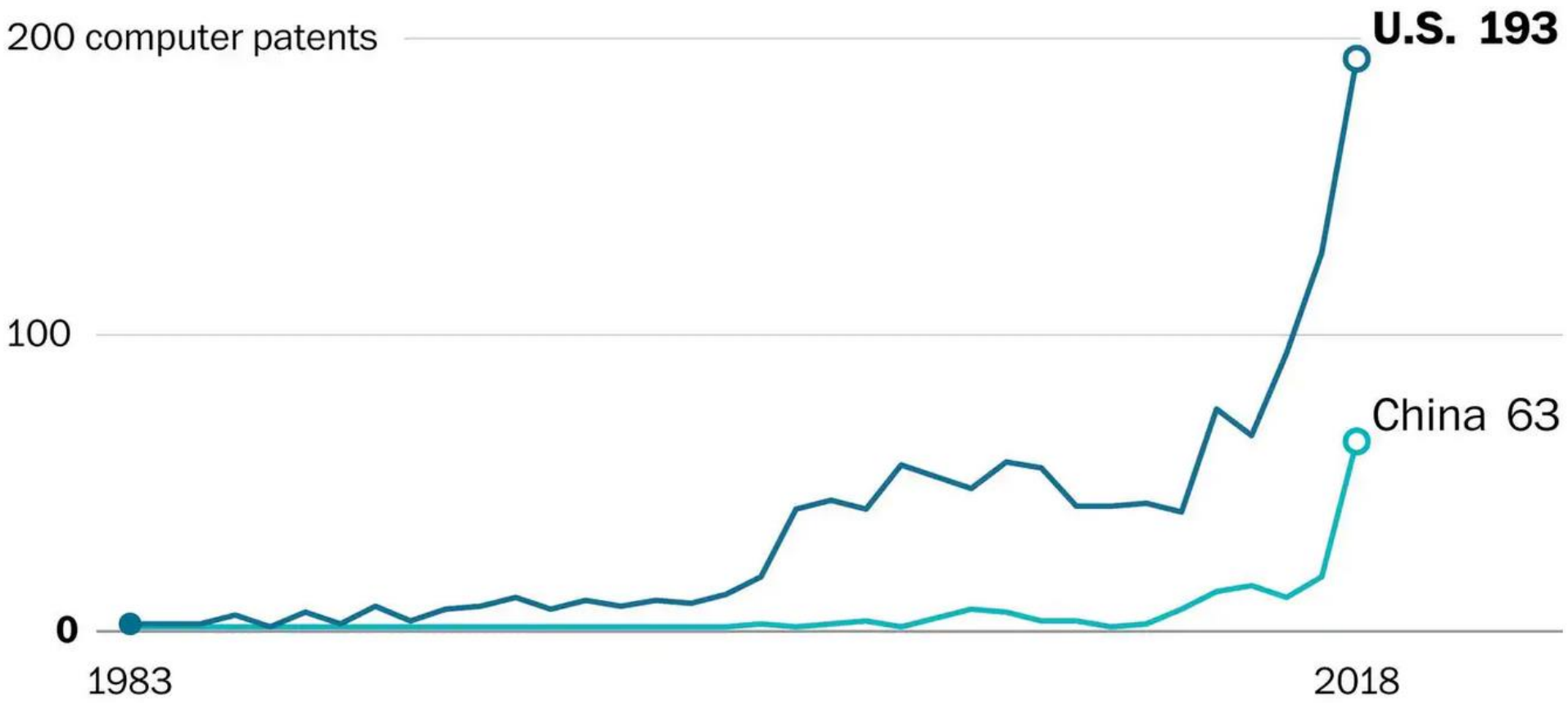
—Xi Jinping, General Secretary, Chinese Communist Party

“*If we want to win the struggle for quantum supremacy, we must not be ‘guerrillas’ — necessarily, we must organize a ‘group army.*”

—Guo Guangcan, Key Laboratory of Quantum Information

Patent filings for quantum computers by country

China has overtaken the United States in quantum technology patents overall, but the United States still has a large lead in patents for quantum computers.

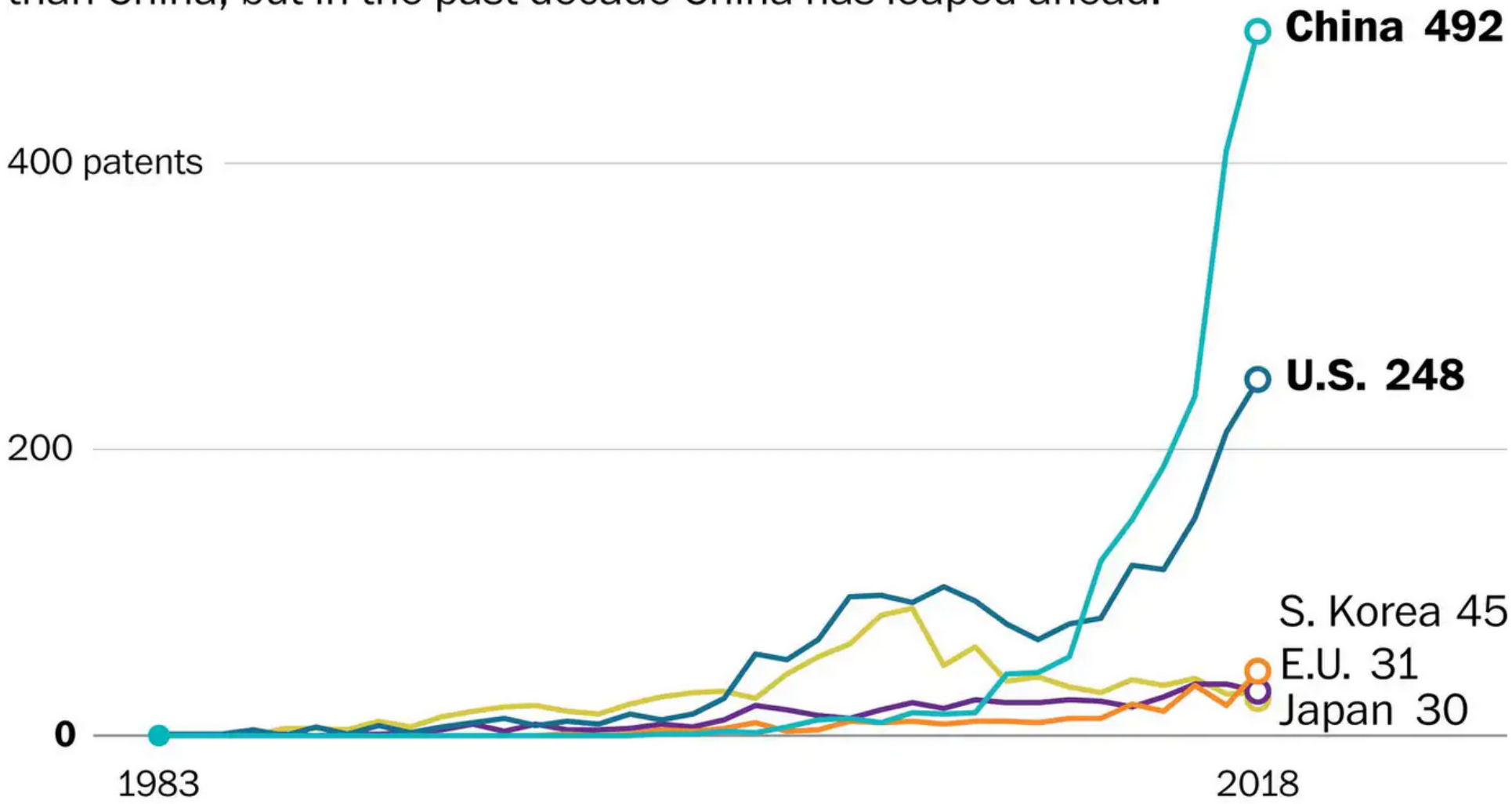


Source: Patinformatics LLC

THE WASHINGTON POST

Patent filings for quantum technology by country

The United States used to produce more patents for quantum technology than China, but in the past decade China has leaped ahead.



Source: Patinformatics LLC

THE WASHINGTON POST

Thank you.

Questions?

@EBKania

EKania@cnas.org