Quantum Computing

Warm-up

Have you heard of quantum computing before? Think about how it could impact society.

I. Listen to the text and practice shadow-reading. If you want, get ready to read it out loud in class in the reading competition.

Why you can't ignore quantum computing

You can't afford to ignore quantum computing. Encryption needs to be updated to protect sensitive data.

Quantum technologies, which take advantage of the strange fuzziness of the subatomic realm, will have a profound impact on our society—from medicine and materials science to banking and clean energy. Such technologies, which include communications, computing, quantum sensing and simulation, will bring many benefits. But they will also make necessary a dramatic shift in the global cyber-security architecture—a process that will start in earnest during 2023.

Quantum computers are still in development. But as they become more powerful and more reliable, they will pose a threat to how we transmit and store confidential data including bank transactions, sensitive government information and intellectual property. That is because unlike existing computers, quantum computers will be able to crack the encryption systems that provide secure data communication and storage, and underpin the global economy.

Criminals and other adversaries know that this will be possible one day—and they are not waiting to get their hands on sensitive data. They are already carrying out "store now, decrypt later" (SNDL) attacks—stealing data for future decryption with quantum computers. According to America's Department of Homeland Security, the decryption of this data could be feasible as soon as 2030. If this happens, any encrypted data acquired by adversaries today will have a maximum confidentiality period of eight years.

Criminal groups are targeting intellectual property and other kinds of data that will keep their value years from now when they decrypt it. This means that as quantum computers scale, there will be "submarine decryptions'' of data troves that will surface unexpectedly, just like submarines in water.

This is not a tomorrow problem: SNDL attacks are being perpetrated right now. Once stolen, there is no way to protect encrypted data. For example, an aerospace company could lose billions in future revenue if its proprietary designs are stolen. A government's military and intelligence operations could be compromised if plans fall into an adversary's hands. (Several countries are actively engaged in building quantum-computing hardware for the sole purpose of defeating public-key cryptography and securing their own critical systems and data.)

In response, researchers have in recent years developed quantum-resistant cryptographic schemes—new forms of encryption that even future quantum computers will be unable to crack. These are known collectively as "post-quantum" cryptography (PQC).

In July 2022 America's National Institute of Technology and Standards (NIST) announced the results of a six-year, multinational process to set the new PQC standards. Experts from more than 25 countries participated in developing and validating these algorithms. NIST also launched a

National Cybersecurity Centre of Excellence, composed of 12 leading companies from around the world, to develop PQC migration strategies and models for future hardware and software solutions.

With this watershed event, governments, corporations and technology providers finally have the clarity and certainty they need to begin the transition to PQC. The next two years will be critical as governments and corporations begin that process.

Identifying all the devices and systems that need to be upgraded, working out which of the multiple NIST algorithms should be deployed in each case and making systems "crypto-agile" (i.e. easily upgraded in the future) is a daunting task that will take several years. More than 20bn devices globally need PQC software upgrades—every mobile phone, laptop, desktop, server, website and mobile app—plus additional systems built into cars, ships, planes and operational infrastructure.

For this reason, 2023 will be a pivotal year for cyber-security and the emerging quantum-technology ecosystem. Driven by the need to protect against immediate and emerging threats, it is the year when public and private entities will start the process of migration.

The cyber-security risk has a silver lining: it will create awareness and drive adoption of quantum technologies in other areas. Forward-looking companies in financial services, health care, pharmaceuticals, telecommunications, transport, defence and other industries will explore the potential for quantum computing to accelerate R&D, enhance their offerings and bring new innovations to market—in 2023 and beyond.

II. Write English collocations from the text for the following ones in Russian.

квантовые технологии	quantum technologies
квантовое зондирование	quantum probing
квантовое моделирование	quantum modeling
квантовые вычисления	quantum computing
представлять угрозу для	to cause danger
непосредственные и возникающие угрозы	immediate and emerging threats
конфиденциальные данные	confidential data
конфиденциальная информация	confidential info
интеллектуальная собственность	intellectual property
взламывать системы шифрования	crack encryption systems
безопасная передача данных	
хранение данных	data storing
зашифрованные данные	crypted data
массивы данных	data arrays / troves
собственные разработки	property designs
военно-разведывательные операции	military and intelligence operations
переломное событие	curcular / watershed event / point
постквантовая криптография	PQC
криптогибкие системы	crypto agile
сложная задача	daunting task
мобильное приложение	mobile app
обновления программного обеспечения	software updates
государственные и частные организации	public and private entities
перспективная компания	forward-looking companies

III. Translate the following phrases using lexical chunks from the text.

получить доступ к конфиденциальным данным	
попасть в руки злоумышленника	
расшифровка с помощью квантовых компьютеров	
решающий год для кибербезопасности	
стимулировать внедрение квантовых технологий	
иметь и положительную сторону (позитивный момент)	
выводить на рынок инновационные продукты	

IV. True or false?

F 1. Quantum computing will have no impact on our society.

F 2. Quantum technologies include only quantum computing.

F 3. Quantum computers are already powerful and reliable.

F 4. Existing computers can crack the encryption systems that provide secure data communication and storage.

T 5. Criminals are waiting for quantum computers to crack encryption systems.

P 6. The decryption of data stolen by criminals could be feasible as soon as 2023.

F 7. Criminal groups are not targeting intellectual property and other kinds of data that will keep their value years from now when they decrypt it.

T 8. Researchers have not developed quantum-resistant cryptographic schemes.

T 9. Post-quantum cryptography (PQC) is a new form of encryption that even future quantum computers will be unable to crack.

T 10. The transition to PQC will take several years.

V. Answer the following questions:

1. What is quantum computing and how will it impact society?

2. Why do existing encryption systems need to be updated, and what threat do quantum computers pose to data security?

3. How are criminals already taking advantage of the potential for quantum decryption, and what is the timeline for this technology becoming a reality?

4. What kinds of data are being targeted by criminal groups in anticipation of future quantum decryption capabilities?

5. What are some potential consequences of sensitive data falling into the wrong hands due to quantum decryption?

6. What is post-quantum cryptography (PQC), and how does it differ from traditional encryption methods?

7. What was the result of America's National Institute of Technology and Standards' six-year process to set new PQC standards?

8. What challenges will governments and corporations face in transitioning to PQC, and how long will this process take?

9. Why is 2023 a pivotal year for cyber-security and the emerging quantum-technology ecosystem?

10. In addition to improving cyber-security, what other benefits might quantum technologies bring to industries like finance, healthcare, and defense?

VI. Be ready to discuss in pairs the potential benefits and risks of quantum computing.