



Co-funded by
the European Union



ВЪВЕДЕНИЕ В КВАНТОВАТА КОМУНИКАЦИЯ



Project: BG National QCI Plan – 101091399
Digital Europe Programme

СЪДЪРЖАНИЕ

- Какво е класическа криптография
- Какво е квантова комуникация
- Защо е нужна квантовата комуникация
- Какво е квантово разпространение на ключове
- Какво представлява EuroQCI
- Какъв е Националният QCI план на България

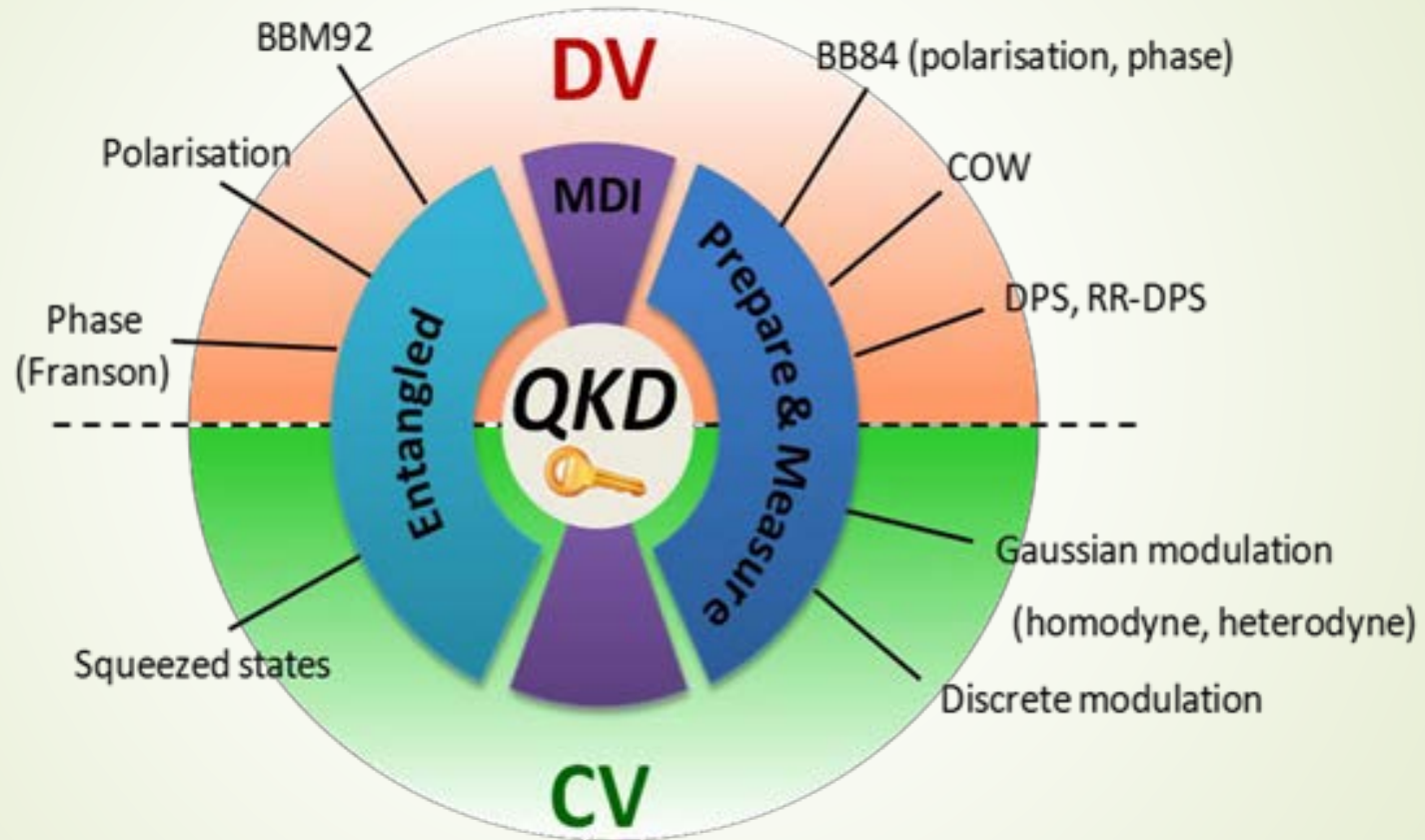
Класическа криптография

- Шифър на VERNAM (неразбиваем):
one-time pad - симетрична криптография – един и същи ключ за криптиране и декриптиране (случаен)
- **Advanced Encryption Standard (AES-256)**: симетричен ключ, генериран по сложен детерминистичен алгоритъм
- **Public Key Cryptography**: двойка публичен и секретен ключ познавайки секретния **САМО ТИ** можеш да дешифрираш съобщение криптирано с публичния ключ
- **Сигурност**: сложни математически задачи отнемат време

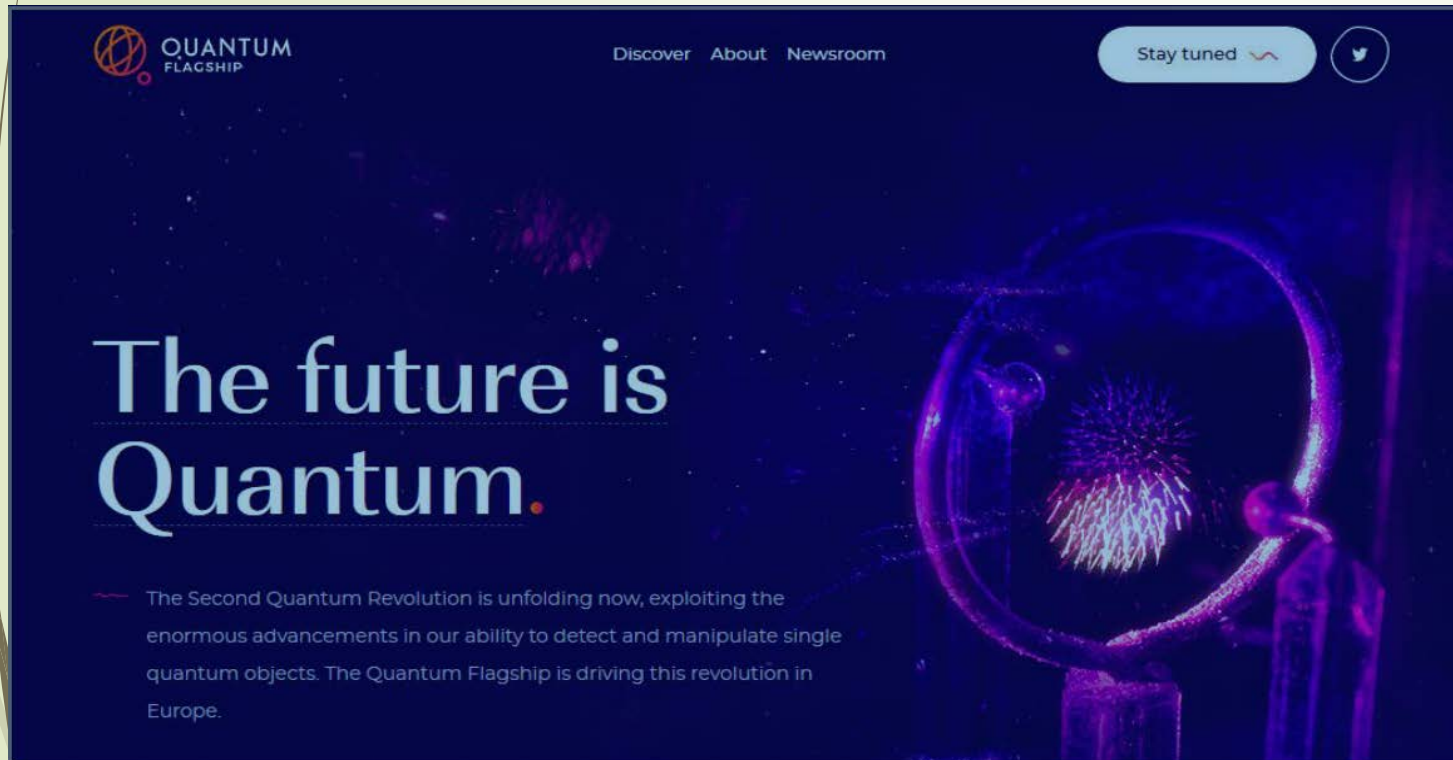
Квантова комуникация

- Класически шифър на VERNAM (one-time pad)
- **Алгоритъм (протокол):** за разпространение на ключа, изп. **квантовите** свойства на фотоните-поляризация
- Оптични влакна, free-space, сателити на ниска земна орбита
- **Сигурност:** 100% стохастичен ключ (квантов генератор на случайни числа), забрана за копиране квантовото състояние на единични фотони, всяко подслушване (частично или пълно) поврежда ключа; Alice и Bob забелязват намесата; съотношения на неопределеност на Хайзенберг, сплетени квантови състояния на двойки фотони

QKD протоколи



Втората Квантова революция



QUANTUM FLAGSHIP Discover About Newsroom Stay tuned

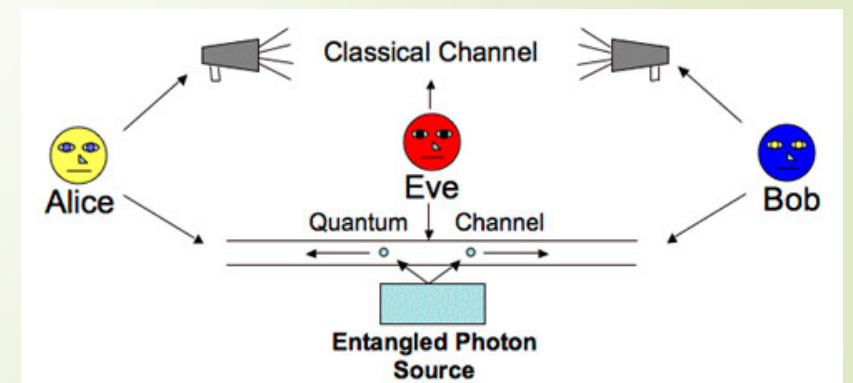
The future is Quantum.

The Second Quantum Revolution is unfolding now, exploiting the enormous advancements in our ability to detect and manipulate single quantum objects. The Quantum Flagship is driving this revolution in Europe.



Quantum Flagship in a nutshell.

- 01 **1b €**
Quantum Technology will be funded with at least one billion Euro by the European Commission.
- 02 **10+ yrs**
Flagship's timescale
- 03 **5000+**
researchers residing in all EU and associated countries involved
- 04 **140**
Research and Innovation Actions (RIA) proposals submitted in response of the first Quantum Flagship call



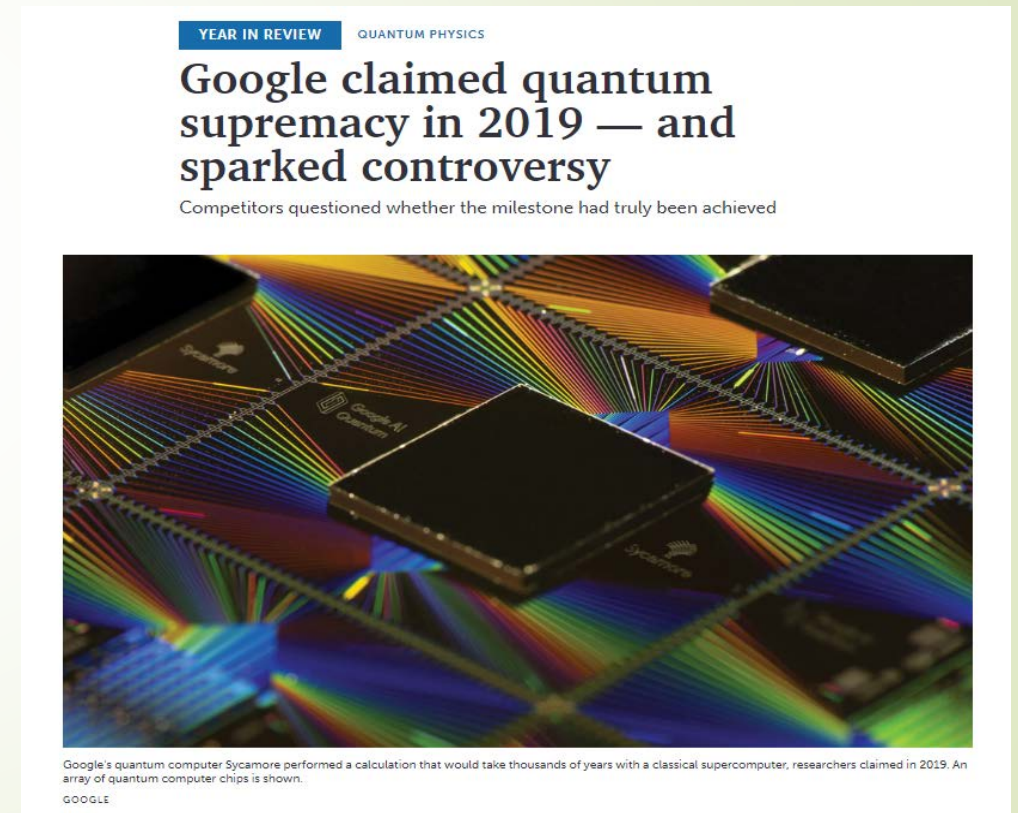
Защо се изгражда QCI¹?

Заплахата от квантовите компютри е реална !

През 2019 Google показа квантови изчисления в рамките на 200 сек. , които биха отнели на класически суперкомпютър 10 000 г.

През м. декември 2020 китайски квантов компютър демонстрира превъзходство от 10^{14} пъти спрямо класическите суперкомпютри.

¹Quantum Communications
Infrastructure



Source: ScienceNews.org

Защо се изгражда QCI¹?

Заплахата от квантовите компютри е реална !

През м. декември 2022 г. китайски изследователи твърдят, че са намерили начин да разбият 48-битов RSA ключ използвайки квантов компютър с 10 кубита.

Твърдят, че са нужни 372 кубита за да разбият 2048-битов RSA (през 2025?)

Title: "Factoring integers with sublinear resources on a superconducting processor"

Времето необходимо за класически суперкомпютър = Възрастта на Вселената; За квантов компютър (с алгоритъма на Shor) = часове или дни за свръхпроводящ процесор

¹Quantum Communications Infrastructure

Quantum technologies [+ Add to myFT](#)

Chinese researchers claim to find way to break encryption using quantum computers

Experts assess whether method outlined in scientific paper could be a sooner-than-expected turning point in the technology



A silicon wafer of quantum computer chips made by Hitachi © Yoshio Tsunoda/AFLO

Richard Waters JANUARY 5 2023 143

Source: arxiv.org, ft.com

Nature (2023) vol. 624(7991), p. 238

The image is a screenshot of a web browser displaying a Nature journal article. The browser's address bar shows the URL: <https://www.nature.com/articles/d41586-023-03854-1>. The Nature logo is prominently displayed at the top left of the page. Navigation links include 'View all journals', 'Search', and 'Log in'. A secondary navigation bar contains 'Explore content', 'About the journal', 'Publish with us', 'Subscribe', 'Sign up for alerts', and 'RSS feed'. The article breadcrumb is 'nature > news > article'. The date is 'NEWS | 04 December 2023'. The main headline is 'IBM releases first-ever 1,000-qubit quantum chip'. The sub-headline reads: 'The company announces its latest huge chip – but will now focus on developing smaller chips with a fresh approach to ‘error correction’.' The author is 'By Davide Castelvecchi'. Social media icons for Twitter, Facebook, and Email are present. On the right side, there are buttons for 'Access through your institution' and 'Buy or subscribe'. Below that, 'Subjects' are listed as 'Mathematics and computing' and 'Quantum physics'. At the bottom right, there is a 'Sign up to Nature Briefing' button with an envelope icon.

← → ↻ 🏠 🛡️ <https://www.nature.com/articles/d41586-023-03854-1> 📄 ☆ 🔍 Search 📧 ⌚ 📱 🗄️ ☰

nature View all journals 🔍 Search Log in

Explore content ▾ About the journal ▾ Publish with us ▾ Subscribe Sign up for alerts 🔔 RSS feed




[nature](#) > [news](#) > article

NEWS | 04 December 2023


IBM releases first-ever 1,000-qubit quantum chip

The company announces its latest huge chip – but will now focus on developing smaller chips with a fresh approach to ‘error correction’.

By [Davide Castelvecchi](#)


IBM has unveiled the first quantum computer with more than 1,000 qubits – the

 Access through your institution

Buy or subscribe

Subjects

[Mathematics and computing](#) [Quantum physics](#)

Sign up to Nature Briefing 



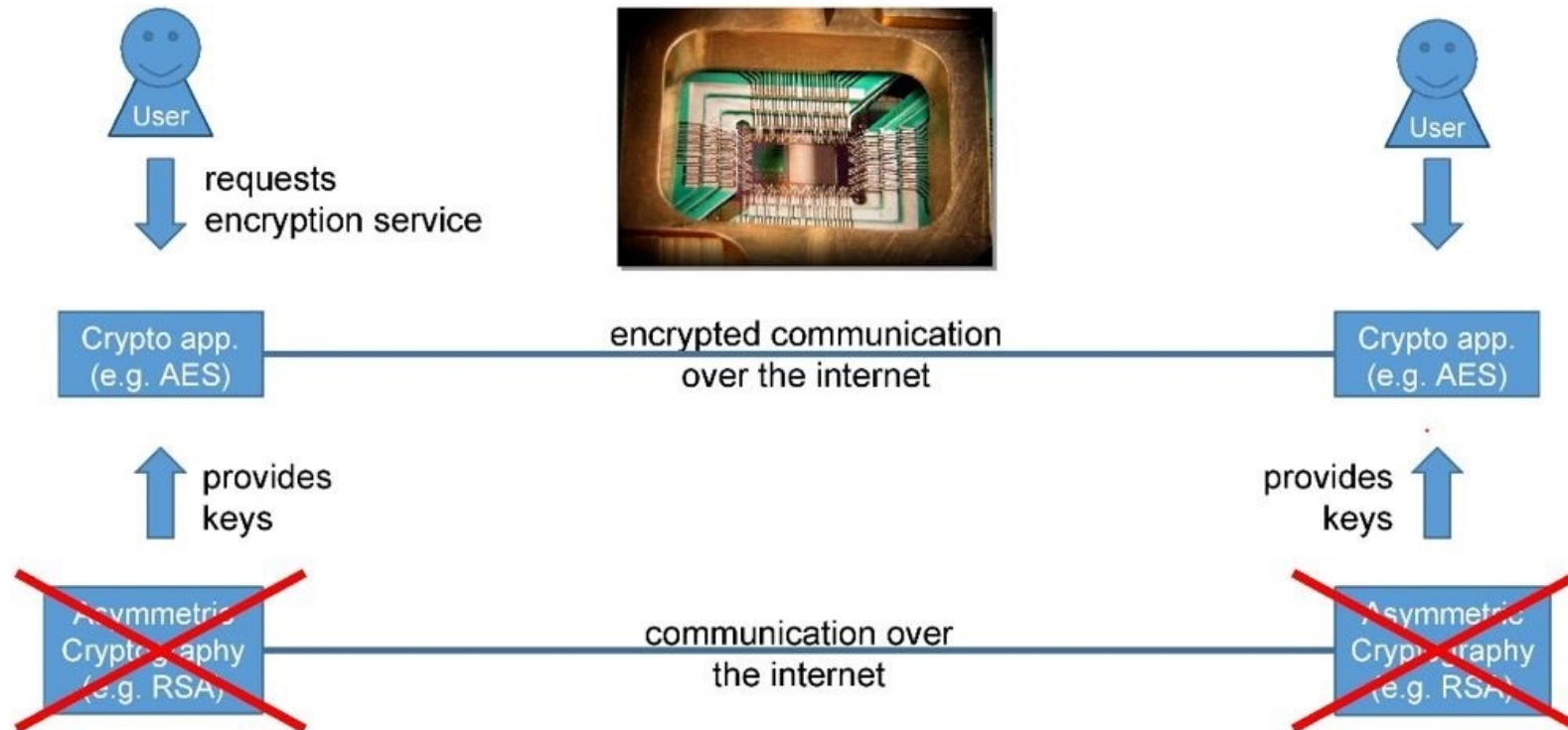
QKD скептици: „Не е ли твърде рано?“ HNDL attack

Harvest Now, Decrypt Later (HNDL) attack

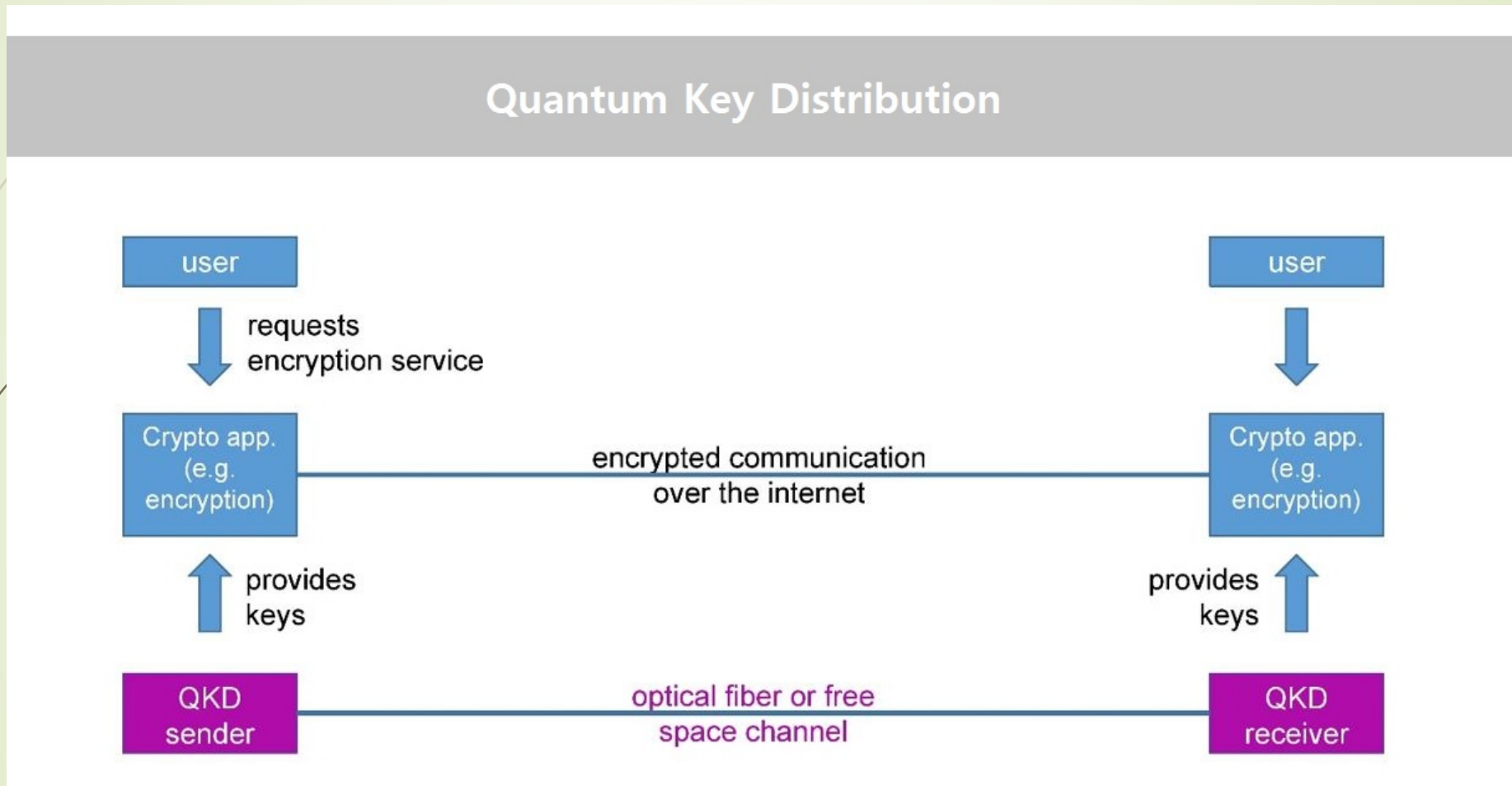
Напомняне: проект VENONA в САЩ събира през периода 1943-1945 стотици хиляди шифрограми (one-time pad) от СССР до САЩ но ги дешифрира едва след 1946 г., когато вече притежават кодова книга на СССР (35 000 дублирани)

Квантова комуникация

The threat of quantum computers



Какво е квантова комуникация?



Какво е EuroQCI



- м. юни 2019 (7 MS): Декларация за внедряване на **European Quantum-secure Communication Infrastructure**
- м. февруари 2020: България подписва Декларацията
- 2021: Всички 27 Държави Членки на ЕС вече са подписали Декларацията и са част EuroQCI

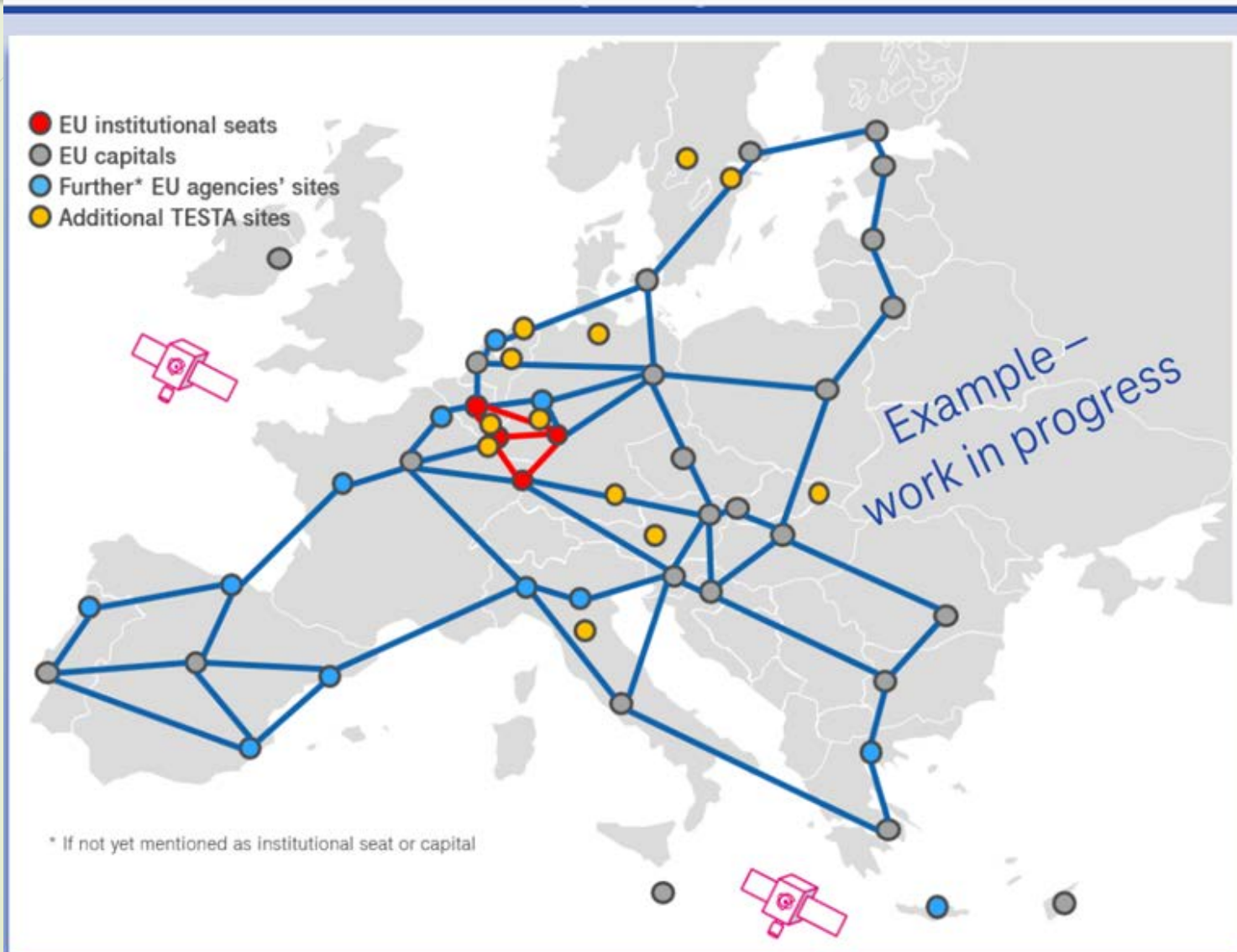


EuroQCI Action Plan: първа фаза

2023-2025 научно-изследователска фаза: preparatory/first deployment phase

- Развитие и внедряване на Европейски технологии за QKD;
- Първоначално внедряване на експериментални квантови мрежи комбинирайки най-добрите класически и квантови технологии в рамките на националните планове за QCI;
- Развитие на първите тестови трансгранични квантови наземни мрежи свързващи съседни национални QCI мрежи чрез “trusted nodes”;
- Развитие на първите тестови оптични наземни станции за връзка между космическия и наземния сегмент на QCI;
- Изграждане на пан-европейска инфраструктура за тестване и валидиране за осигуряване на доверие в EuroQCI;

Карта на паневропейската мрежа EuroQSI при успешна реализация на първия етап от Плана за **ДЕЙСТВИЕ** на EuroQSI до края на 2025 г.





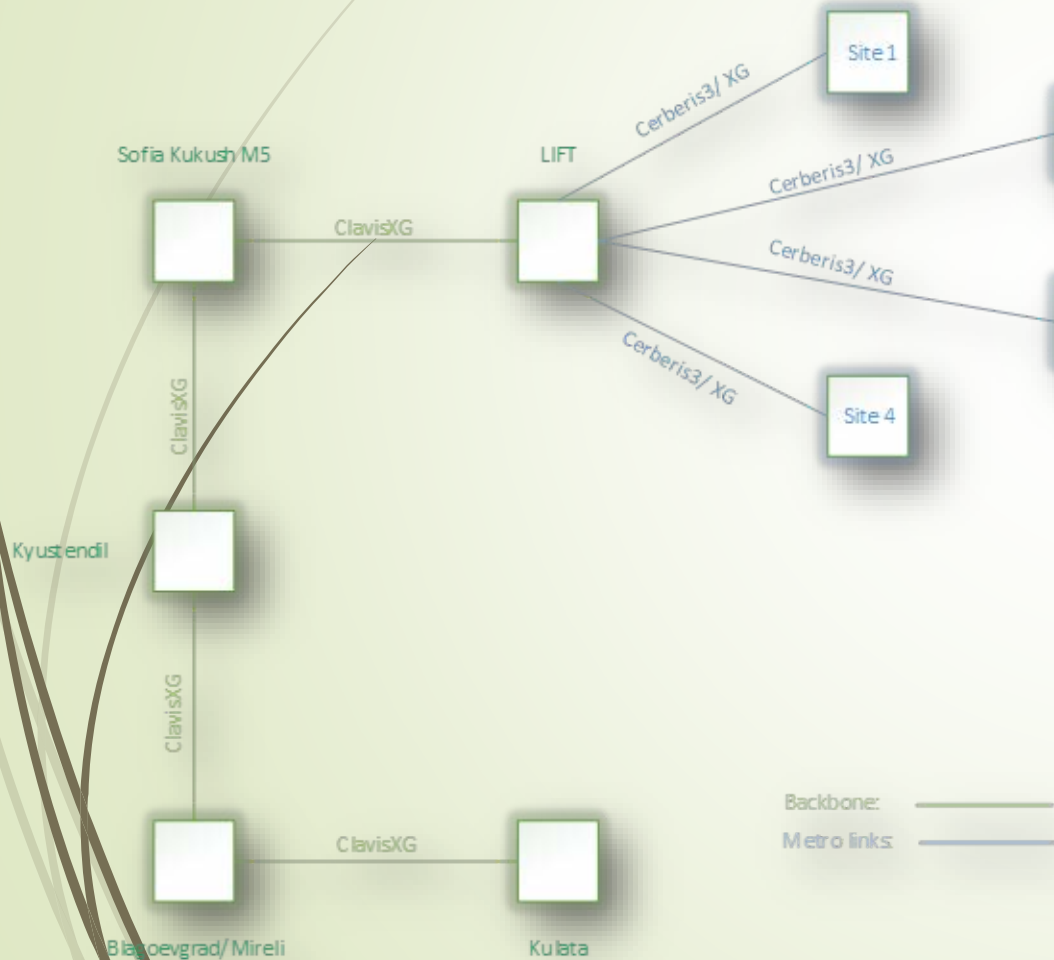
Национален план за QCI

Потенциални сфери на приложение на QCI в България:

- ▶ Електронно управление
- ▶ Международна и вътрешна сигурност
- ▶ Икономика и Финанси, Регионално развитие
- ▶ Електроразпределение, комуникации и транспорт
- ▶ Медицина и здравеопазване
- ▶ Социална политика
- ▶ Високотехнологична индустрия и др.

Партньори в Българския консорциум

BG National QCI Plan: телеком оператори и компании свързани с тях



Водещ партньор: CoC QUASAR
Институт по роботика - БАН



Enterprise Communications Group



Electron Progress



Correct Consulting Group

Асоциирани партньори

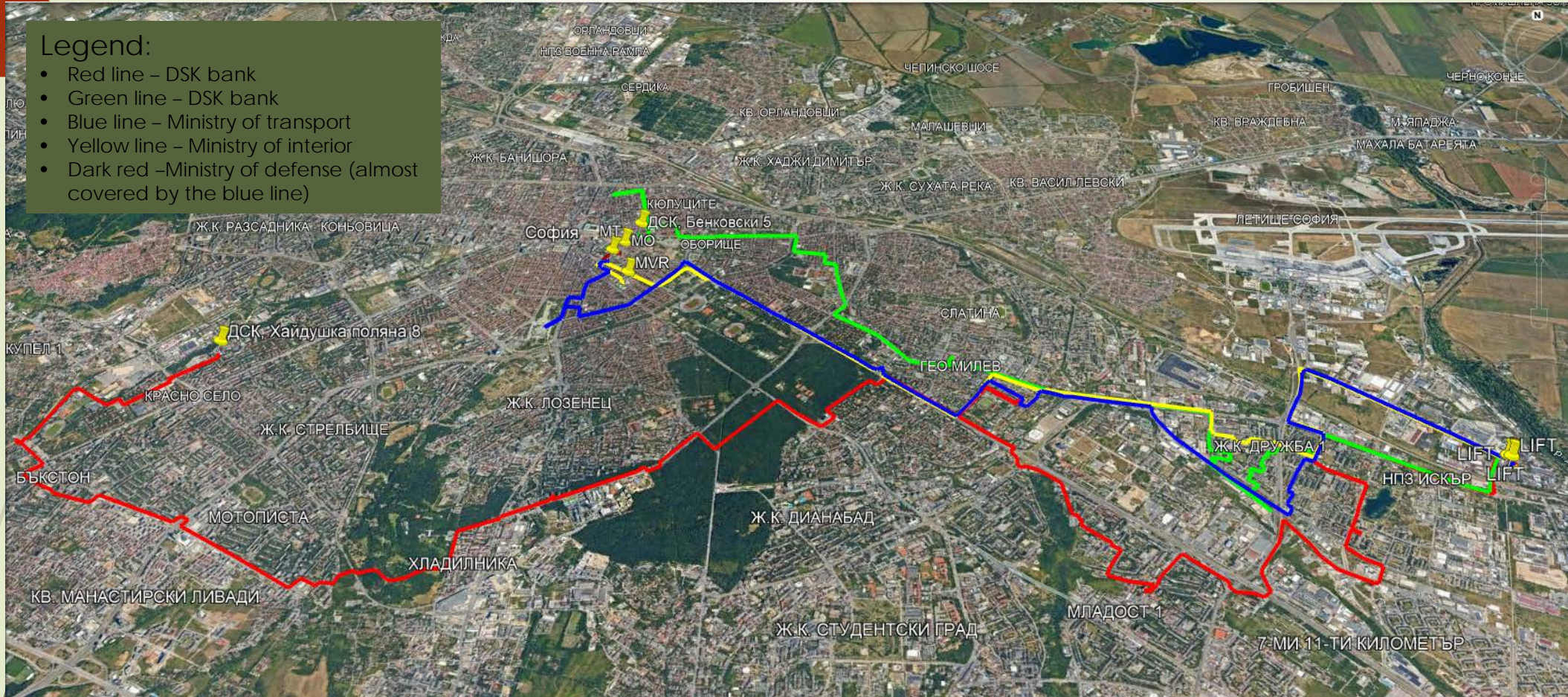
Министерство на отбраната, МВР,
Министерство на транспорта, ДАНС,
Софийска община, Банка ДСК



SOFIA METROPOLITAN NETWORK

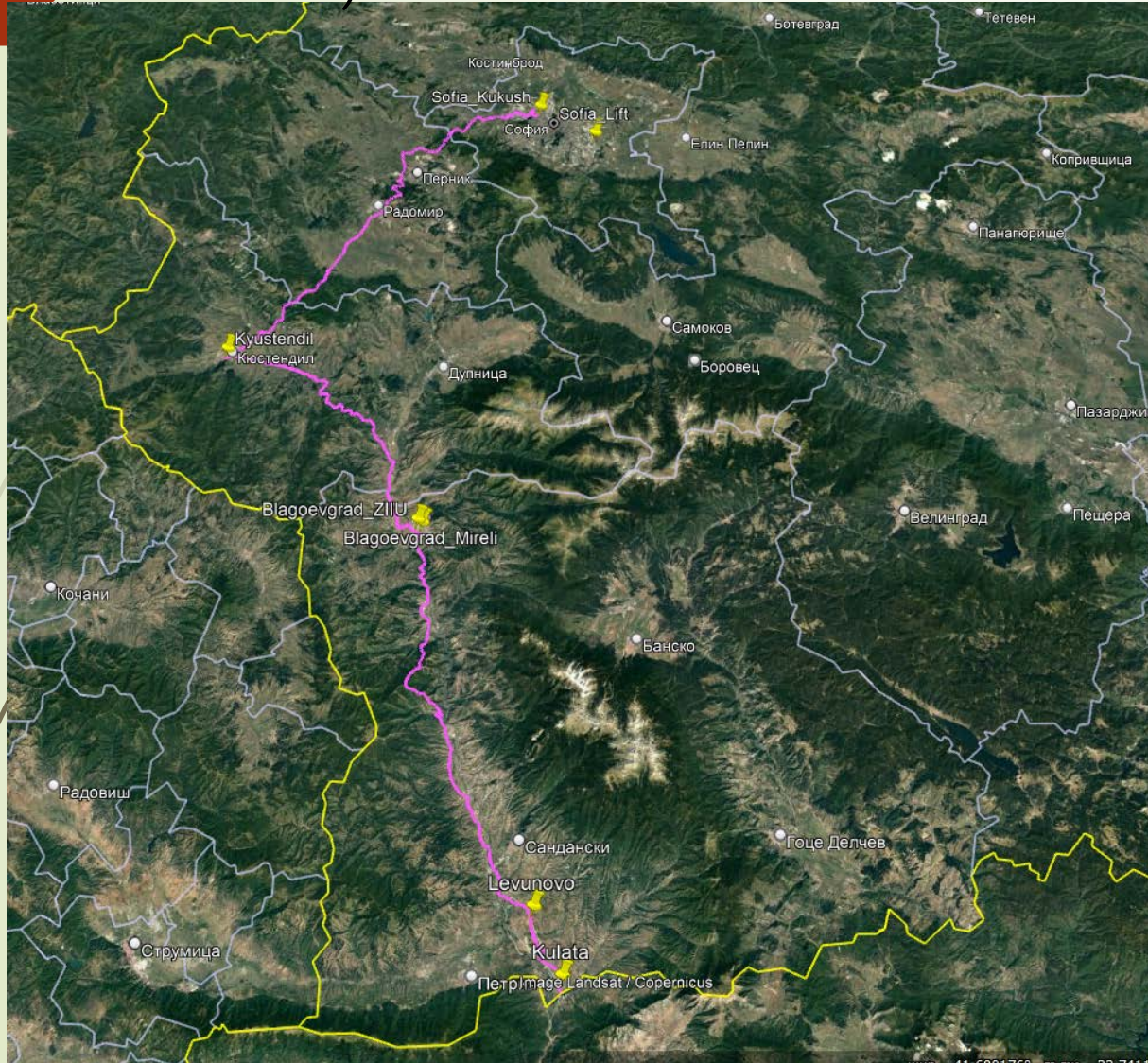
Legend:

- Red line – DSK bank
- Green line – DSK bank
- Blue line – Ministry of transport
- Yellow line – Ministry of interior
- Dark red – Ministry of defense (almost covered by the blue line)



- Optical fibers almost prepared – running fibers into the ministries' buildings still in progress
- High level design prepared
- Laboratory tests with rented equipment performed
- Access procedures in progress
- Discussions with the ministry representatives about technical details – what and how could be protected in their networks with this technology

LONG-DISTANCE PART OF THE PROJECT **SOPIA-KULATA** (BG-GR BORDER)



- Prepared the optical sections for the long-distance part
- Site surveys made
- Prepared the colocations (trusted nodes)
- Carried out tenders for the equipment
- Contracts signed
- Provided optical fiber characteristics to the QKD equipment provider
- Contracts for the equipment signed
- Equipment produced
- High level design elaborated
- Equipment delivered
- Low level design is in progress
- Laboratory tests of the equipment forthcoming
- Planning site installations



**Благодаря за
вниманието!**