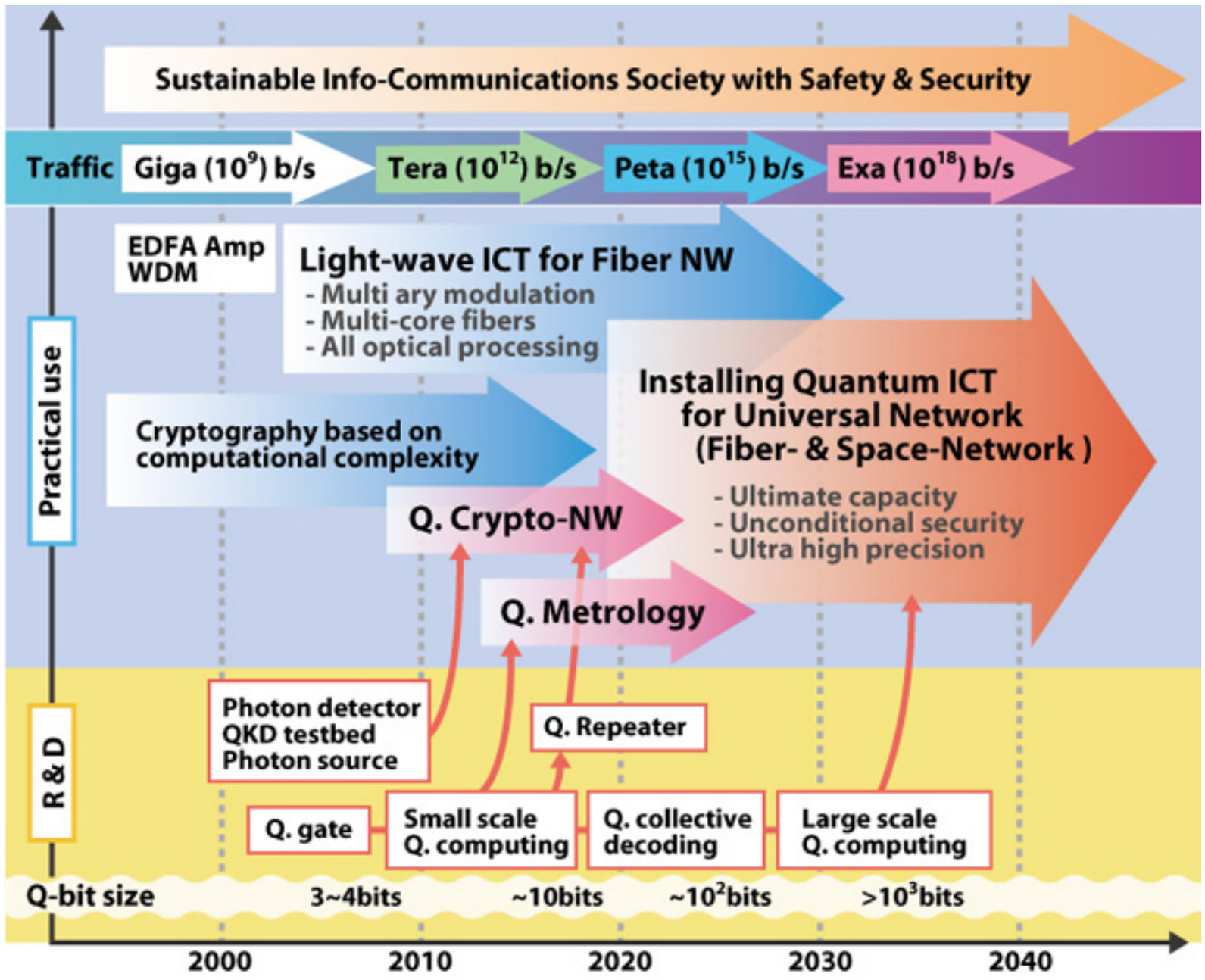
Road Map



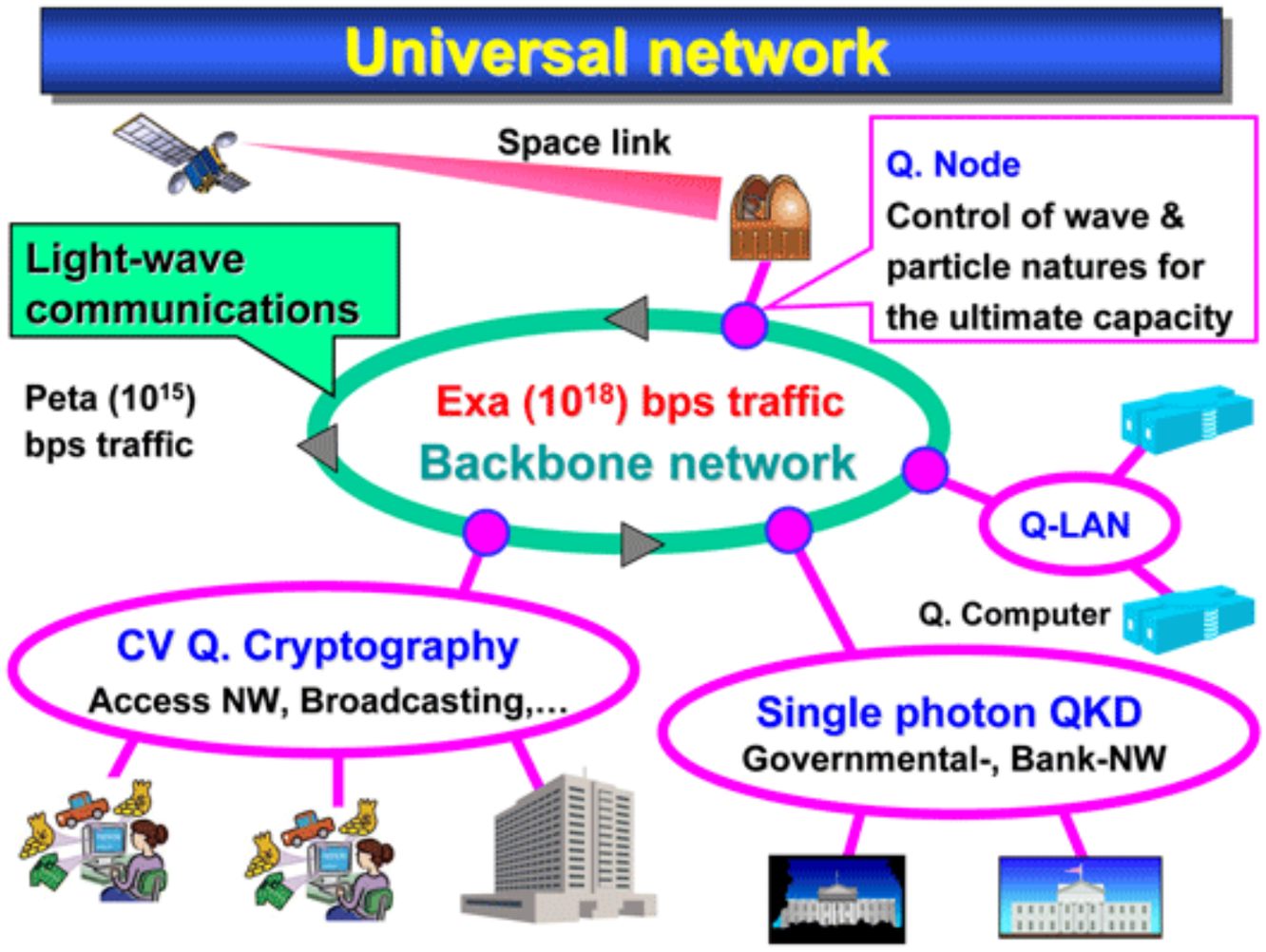
Optical communications are utilizing full potential of the wave nature of light by controlling amplitude and phase for every available modes. This kind of light-wave ICT continues to sustain the increasing capacity demand for future network over a few decades, realizing the network traffic of Peta (1015) b/s.

On the other hand, the information security, which is a more urgent demand, is now ensured by cryptography based on computational complexity of mathematical problems. But this will not last unfortunately. Actually they are always threatened by technological advancement.

Quantum cryptography provides a mean to ensure the information security by the laws of quantum mechanics. Several protocols of quantum key distribution (QKD) such as BB84 and BBM92 have been certified by the unconditional security proofs, which means even any technologies cannot hack them. Fortunately this is within the reach of recently developing technology of single photon detector. So the first application of quantum infor-communications technology (Q-ICT) is QKD technologies in 4 years, which are especially for government chartered networks and bank networks.

The next application of Q-ICT will be quantum metrology, such as a new clock and optical sensing, using small scale quantum computing. They will start to be used in particular institutes and companies after 2010. Quantum repeater, which is a key to extend QKD network and also quantum-enhanced network, is a bit challenging technology, and it will take another decade for practical use.

In 15 years, installing various Q-ICTs to fiber- and space-network will begin. When large scale quantum computing is realized, we can realize the universal network with the ultimate capacity, the unconditional security, and the ultra high precision.



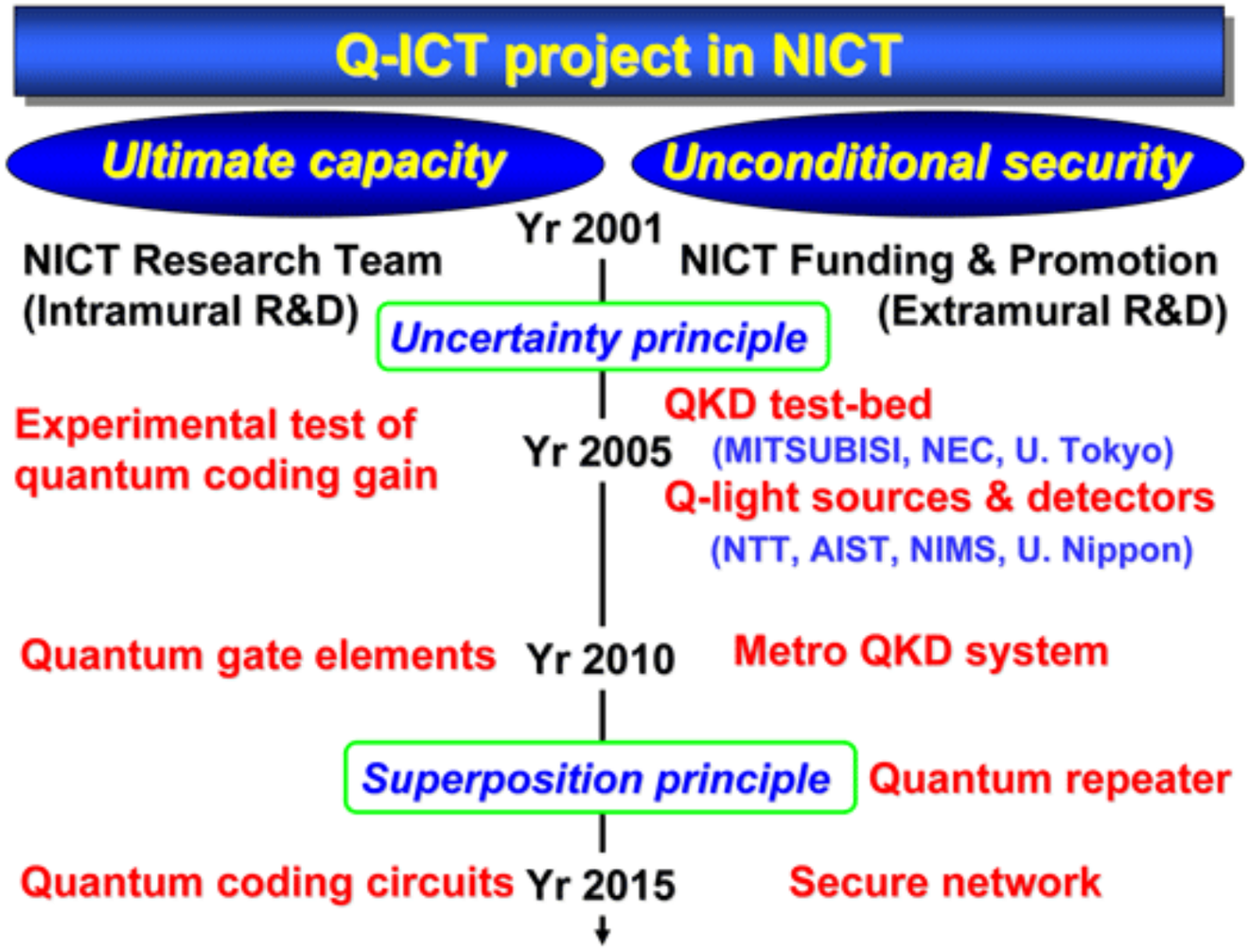
Light-wave ICT will continue to be a core technology to sustain backbone networks in any era. Q-ICT will be used to enhance the light-wave ICT network for the ultimate performance.

Quantum cryptography will realize the ultimate information security. There are two kinds of implementations: continuous variable (CV) quantum cryptography based on coherent states & homodyne detection, and single photon QKD. Complete proof of the unconditional security of CV schemes is still open, but it can realize robust information security against a wide range of attacks. More importantly this is within the reach of today’s technology of light-wave ICT.

Unconditionally secure cryptography can be realized by controlling particle nature of light, namely, it is possible to impose more stringent constraints on eavesdroppers by using the minimum quanta, “photons.“ Famous examples of unconditionally secure QKD protocols are BB84 & BBM92.This is within the reach of recently developing technology of single photon detector. CV quantum cryptography is more likely to be used for ensuring information security in access network and broadcasting on it. In these applications, the unconditional security is not necessarily the first demand, but more high speed operation and usability are a primary concern. Single photon QKD is, on the other hand, expected to be used for government-chartered NW and bank NW.

More advanced Q-ICT includes quantum entanglement control, quantum teleportation with it, and small scale quantum computing. This also includes photon number resolving detectors as a basic element. They can be assembled to realize a truly quantum network linking quantum computers, the so-called quantum local area network (Q-LAN).

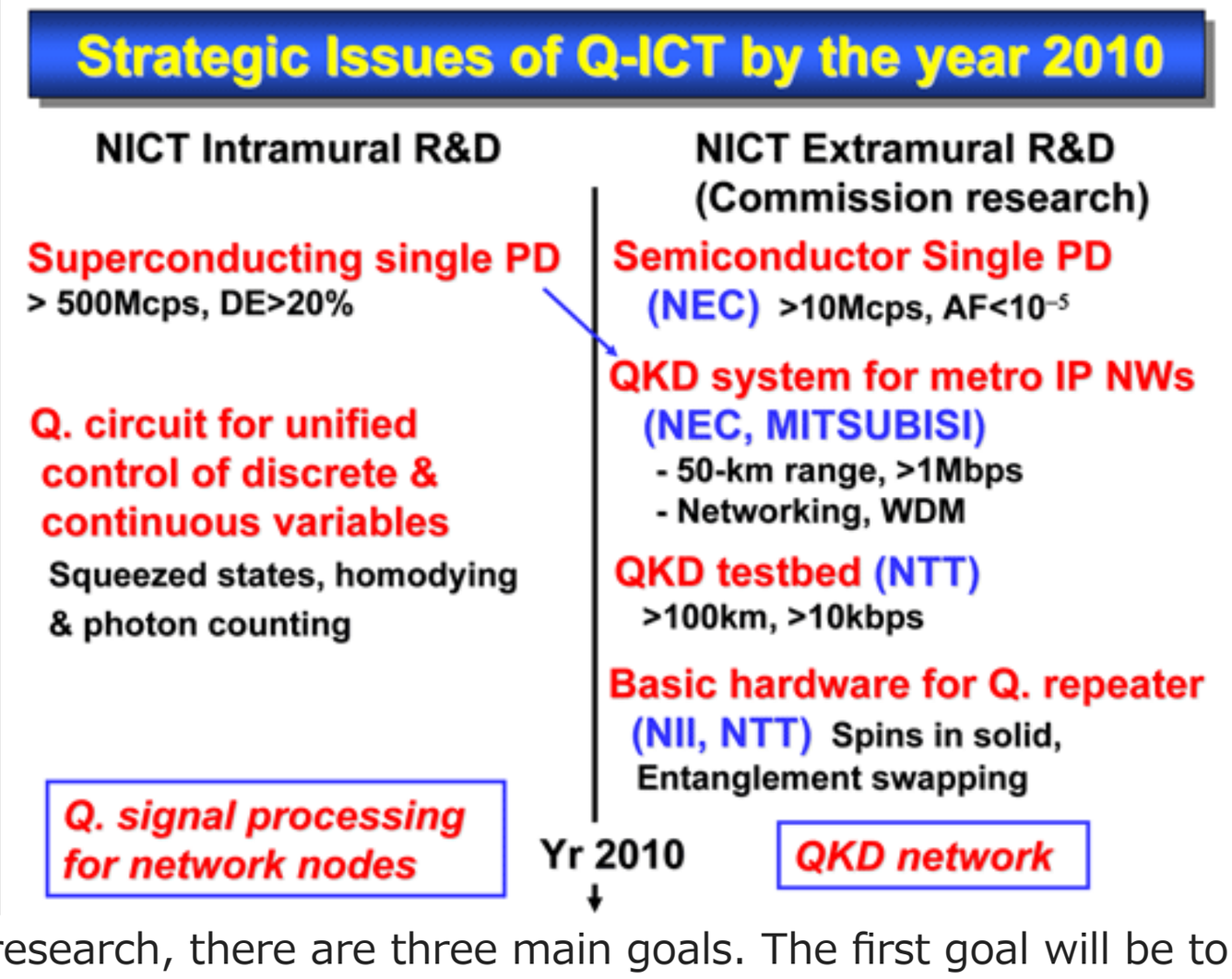
When large scale quantum computing is realized, and combined with interface to photons, they can be used to control both wave and particle natures of light for the ultimate capacity. This level of technology will eventually be used in the network nodes,to attain the ultimate capacity in a range of exa bps and higher. In such quantum nodes, universal quantum optical operations are performed on the coherent states, which are the main signal carriers in the backbone network, for example, to generate their quantum superposition states, the so called Schroedinger’s cats. Those have been known as a famous paradox in quantum mechanics. Our research is revealing that they will not be a paradox any more, but a key to realize the ultimate ICT.



Quantum Info-Communications Technology (Q-ICT) project in NICT has started in 2001. Its mission is to provide technological foundations for unconditional security and ultimate capacity.

For unconditional security, NICT promotes development of quantum key distribution (QKD) systems, and related basic technologies, by funding private & public organizations. The commission research teams for the past five years (2001-2005) were Misubishi Electric Co Ltd, NEC, University of Tokyo, working on QKD systems, NTT working on entangled photon source for fiber network, National Institute of Informatics, National Institute of Materials Science and University Nippon working on quantum light sources and detectors at C-band.

For the ultimate capacity, one should be able to control the superposition principle, which is still far from practical use. This kind of high risk target is pursued by NICT intramural research team.



In the commission research, there are three main goals. The first goal will be to develop a QKD system for metropolitan IP networks within the 50-km range at a minimum key generation rate of 1 Mbps. Networking and WDM technology will also be applied. The second goal is to construct a QKD system exceeding 100 km range at a key generation rate of 10 kbps or higher. The third goal is to develop basic hardware for quantum repeater, by National Institute of Informatics, and NTT. Nuclear spins and electron spins in solid will be exploited for the scalability, and entanglement swapping will be demonstrated.

NICT research team is to provide SSPD to these teams, and will combine all these technologies to realize QKD networks. In a long term, NICT research team is also working on quantum optical circuit for

unified control of discrete and continuous variables, using squeezed states, photon counting, and homodying.

This would eventually be applied to quantum information processing at optical network nodes, to realize the ultimate capacity of optical channels.