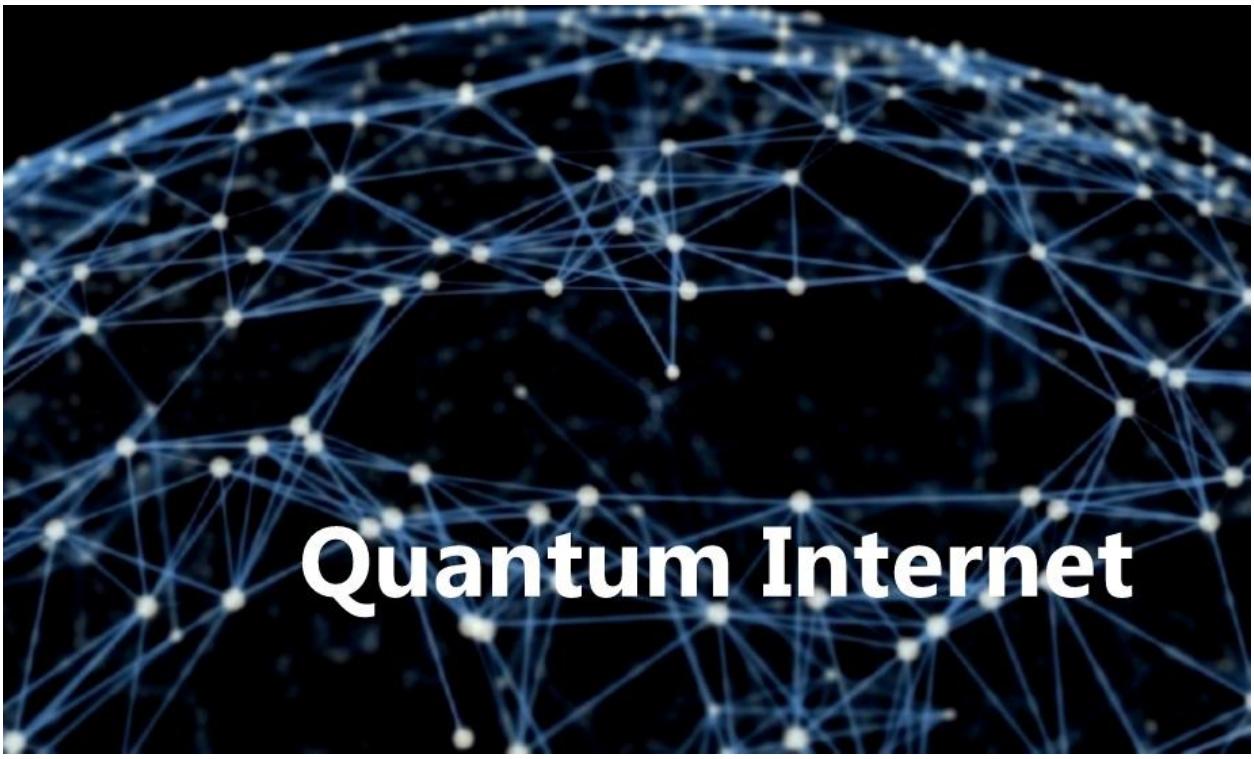
Q-NET



US achieves first uninterrupted quantum internet signal in a major security milestone

This is an important step in creating a quantum internet network that is more secure and capable than existing networks.

Quantum computing uses quantum bits or qubits to store information. Unlike classical binary bits, qubits can exist in more than one state at one time, allowing combinations of physical values to be encoded to a single object. Qubits can also be entangled, transmitting information from one place to another without physically traveling the distance.

Known as quantum teleportation, this is an important component of a quantum-based network. Light particles or photons can be used as qubits in their polarized forms and transmitted using existing fiber-optic cables, much like classical computing data.

However, changes in conditions such as wind, moisture, or even temperature can change the polarization of light and interfere with the signals transmitted. Collaborative research by scientists based at Chattanooga and ORNL worked to address these issues in the existing networks.

Avoiding periodic shutdowns

Joseph Chapman, a quantum research scientist at ORNL, explained that most previous solutions didn't work for all polarization types.

He said in the press, "Most previous solutions didn't necessarily work for all types of polarizations and required trade-offs like periodically resetting the network. People using the network need it up and running."

With Muneer Alshokwan, another research scientist at ORNL, Chapman used automatic polarization compensation (APC) to stabilize the polarization of light waves sent over EPB's commercial-grade fiber-optic network.

APCs can reduce data inference caused by external factors such as wind and temperature. The team used reference signals generated by lasers to check transmitted polarization continuously. This was verified using an approach called heterodyne detection.

"An experienced musician with a good ear can tell the difference when two instruments are out of tune," Chapman added. "In our APC, we're using a laser to do the same thing with our reference signals."

Using entanglement-assisted quantum process tomography, the researchers estimated the properties of the quantum channel. They found that the transmissions remained relatively stable when APC was added, and the noise was minimal.

"Our approach controls for any type of polarization and doesn't require the network to periodically shut down," added Chapman.

The test utilized EPB's fiber-optic commercial quantum network and involved the University of Tennessee Chattanooga and industry partner Qubitekk. Credit: Joe Chapman, Morgan Manning/ ORNL , U.S. Dept. of Energy

.Working towards a quantum internet

Using their approach, the teams successfully transmitted quantum-entangled signals between nodes at the University of Tennessee Chattanooga campus and two other EPB quantum network nodes, each about half a mile away.

"This is the first demonstration of this method, which enabled relatively fast stabilization while preserving the quantum signals, all with 100% uptime – meaning the people at either end of this transmission won't notice any interruption in the signal and don't need to coordinate scheduled downtime," added Chapman.

The researchers have now applied for a patent for their approach. They will work on increasing the bandwidth and compensation to achieve higher-level performance, irrespective of the environmental conditions.

"Working with organizations like ORNL provides valuable feedback on how we can continue to enhance EPB Quantum Network as a resource for researchers, startups, and academic customers," concluded David Wade, EPB's CEO, in the press release.

Imagine a future where internet connections are not only lightning-fast but also remarkably reliable, even in crowded spaces. This vision is rapidly approaching reality, thanks to new research on terahertz communications technologies. These innovations are set to transform wireless communication, particularly as communications technology advances toward the next generation of networks, 6G.

I'm an engineer who focuses on photonics, the study of how light and other electromagnetic waves are generated and detected. In this research, my colleagues and I have developed a silicon topological beamformer chip. Topological refers to physical features in the silicon that help steer terahertz waves, and beamformer refers to the purpose of the chip: forming terahertz waves into directed beams.

Terahertz frequencies are crucial for 6G, which telecommunications companies plan to roll out around 2030. The radio frequency spectrum used by current wireless networks is becoming increasingly congested. Terahertz waves offer a solution by using the relatively unoccupied portion of the electromagnetic spectrum between microwaves and infrared. These higher frequencies can carry massive amounts of data, making them ideal for the data-intensive applications.

Our chip takes a terahertz signal from a single source and splits it into 54 smaller signals, which are then guided through 184 tiny channels with 134 sharp turns. Each beam can transmit and receive data at speeds of 40 to 72 gigabits per second, many times faster than today's 5G networks.

With the help of artificial intelligence, we designed the chip to have a specific microscopic honeycomb pattern to form lanes for the terahertz waves. The array of channels sends out powerful, focused beams that cover the entire 360 degrees around the chip. This allows a phone or other wireless device anywhere around a Wi-Fi router or other communications device to use the chip to receive the high-speed signal. We demonstrated the chip by splitting an input signal of a streaming HD video into four output beams.

Beamformers in wireless networks

Terahertz waves have a shorter range compared with lower-frequency signals used in 4G and 5G networks. Terahertz beamformers address this challenge by precisely directing high-frequency signals to ensure they reach their destination without loss or degradation.

Beamformers are essential for the next generation of wireless communication. Unlike traditional antennas that broadcast signals indiscriminately, beamformers focus signals in specific directions, boosting both efficiency and reliability. Our chip ensures that those beams provide coverage in all directions.

This focused approach not only extends the signal's range but also improves its quality, even over long distances. Beamformers are likely to be crucial in managing stable connections by reducing interference as the world adds billions of connected devices.

A future with terahertz beamforming

The potential impact of terahertz beamforming chips on everyday life is profound. For example, these chips could make it possible to download a 4K ultrahigh-definition movie in mere seconds compared with 11 minutes over today's W-Fi, or support immersive virtual and augmented reality experiences without any lag.

Beyond entertainment, they could make real-time holographic communication a reality, where people appear as lifelike holograms. Smart cities could use this technology to seamlessly coordinate traffic systems and emergency responses, while health care could benefit from remote surgeries where doctors control robotic instruments from afar.

The terahertz beamforming chip represents a significant step forward on the path to faster, more reliable wireless communication by overcoming the challenges of high-frequency signal transmission.

In the world of digital data, and now quantum communication, security has always been a moving target, constantly evolving to meet new challenges.

As technology advances at an unprecedented pace, so do the threats that can compromise our confidential information, making it more crucial than ever to stay ahead of potential attacks.

The rise of quantum computing represents a significant leap in computational power, bringing us to a critical juncture where traditional encryption methods -- once deemed robust -- are increasingly vulnerable to decryption by these advanced systems.

This vulnerability raises serious concerns for businesses and individuals alike, as our reliance on digital platforms grows. But fear not -- quantum key distribution (QKD) is here to revolutionize the way we safeguard our data.

This cutting-edge technology leverages the principles of quantum mechanics to create secure communication channels, ensuring that our information remains protected in ways that were once unimaginable.

By using QKD, we can stay one step ahead of cyber threats and maintain the integrity of our most sensitive data.

Heart of quantum communication

Recently, an exciting experiment in Germany took quantum communication to new heights, representing a big step toward a secure quantum internet.

This achievement was led by Professor Fei Ding from Leibniz University of Hannover, Professor Stefan Kück from the Physikalisch-Technische Bundesanstalt (PTB), and Professor Peter Michler from the University of Stuttgart, along with their brilliant team of researchers.

At the core of this experiment lies a fascinating piece of technology: semiconductor quantum dots (QDs). Often described as "artificial atoms," these

tiny structures hold immense potential in the quantum world, particularly in the realm of quantum information technologies.

50-mile long quantum internet

For the first time, these quantum dots were utilized in an intercity QKD experiment, connecting the cities of Hannover and Braunschweig via optical fiber in what has been dubbed the "Niedersachsen Quantum Link."

"We work with quantum dots, which are tiny structures similar to atoms but tailored to our needs. For the first time, we used these ‘artificial atoms' in a quantum communication experiment between two different cities," noted Professor Fei Ding, explaining the process.

This connection, stretching approximately 79 kilometers (50 miles), forms the first quantum communication link in Lower Saxony, Germany. It's a crucial step towards the realization of a secure, long-distance quantum internet.

Artificial atom (QKD) experiment

The experiment commenced with Alice at Leibniz University of Hannover (LUH), where she prepared single photons encrypted in polarization.

These photons were transmitted through a fiber-optic channel to Bob at the PTB in Braunschweig, whose role was to decrypt the polarized photons using a passive polarization decoder.

This innovative setup successfully illustrated the stable and rapid transmission of secret keys, a crucial element in secure communication.

Quantum communication breakthrough

In an impressive advancement, researchers have confirmed positive secret key rates (SKRs) over distances of up to 144 kilometers, corresponding to a 28.11 dB loss in a controlled laboratory setting.

Over 35 hours, they successfully accomplished high-rate secret key transmission while keeping the quantum bit error ratio (QBER) remarkably low.

Dr. Jingzhong Yang highlighted the importance of this development, noting, "When compared to existing quantum key distribution (QKD) systems that utilize single-photon sources (SPS), the SKR achieved in this study outperforms all current SPS-based implementations."

This significant success not only sets a new benchmark for QKD systems but also underscores the promising potential of quantum dots in various applications within the emerging quantum internet. These include innovations such as quantum repeaters and distributed quantum sensing.

Why we need a quantum internet

The quest for secure communication is intrinsic to human civilization, with its importance magnified in today's digital landscape. As we navigate this era, the stakes have never been higher.

Enter quantum communication -- an incredible technological feat that harnesses the mind-bending properties of quantum physics to deliver unparalleled security.

By utilizing single photons emitted from quantum dot devices, we can transmit information across vast distances with a level of assurance that any interception attempt will be swiftly detected.

"Some years ago, we only dreamt of using quantum dots in real-world quantum communication scenarios," Professor Ding enthused.

"Today, we are thrilled to demonstrate their potential for many more fascinating experiments and applications in the future, moving towards a ‘quantum internet'."

Road ahead for the quantum internet

The successful demonstration of intercity quantum key distribution using semiconductor quantum dots is a glimpse into the future of secure communication.

As we move closer to realizing a quantum internet, the implications for cybersecurity, data privacy, and information sharing are profound.

This experiment lays the groundwork for more extensive and more complex quantum networks that could span entire continents. The integration of quantum dots into these networks is just the beginning.

Researchers speculate that quantum dots could also play a pivotal role in developing quantum repeaters, which are essential for extending the reach of quantum communication networks.

Quantum communication ushers in a new era

As we approach a new era in communication, the work of Professor Ding and his colleagues exemplifies the remarkable potential of innovation and collaboration.

The quantum internet, once a distant aspiration, is now an emerging reality that stands to transform our methods of connection, communication, and the safeguarding of sensitive information.

While the journey to realize the quantum internet is ongoing, each advancement brings us closer to a future where secure communication is not merely a possibility but a certainty.

Though quantum dots may be small, their influence on the future of communication is poised to be profoundly significant.

Imagine the possibility of sending messages that are completely impervious to even the most powerful computers. This is the incredible promise of quantum communication, which harnesses the unique properties of light particles known as photons.

In quantum networks, information is encoded not only in the presence or absence of light pulses, but also in the intricate properties of the photons themselves, such as their polarization.

A pan-European, Asian, and South American research team has developed a new light source that emits exceptionally bright, entangled photons. These special pairs of photons are the cornerstone of quantum communication, a revolutionary technology that promises ultra-secure data transmission. Unlike traditional sources, this new device overcomes limitations by achieving high brightness and entanglement, paving the way for more efficient and secure quantum networks.

A light source that can generate entangled photons is crucial for quantum communication. Entanglement is a bizarre quantum phenomenon where two photons become linked, sharing the same fate regardless of distance. If someone measures the property of one entangled photon, the other instantly reflects that change, even if they're separated by vast distances. This inherent link forms the basis for unbreakable encryption in quantum communication.

However, existing sources for entangled photons often face limitations. Traditional methods, like spontaneous parametric down-conversion (SPDC), can generate high-quality entangled photons but struggle with brightness. This means fewer entangled photons are available for communication, slowing data transfer.

Quantum emitters driven under resonant excitation offer a solution. These emitters can generate photons on demand and have the potential to be much brighter. Among these, semiconductor quantum dots (QDs) are particularly promising. However, until now, scientists haven't been able to optimize both brightness and entanglement in QD sources. They often had to choose between one or the other.

This new research, published in *eLight*, addresses this challenge. The scientists created a unique device integrating a quantum dot with a special light-trapping cavity and a micromachined platform. This allows them to precisely control the properties of the light emitted by the quantum dot. By fine-tuning these properties, they achieved a breakthrough—a source that simultaneously generates bright, entangled photons.

This new source represents a significant step towards practical applications of quantum communication. Generating bright, entangled photons on-demand is essential for building secure and efficient quantum networks. These networks could revolutionize various fields, from ultra-secure communication for governments and financial institutions to unbreakable encryption for everyday transactions.

While challenges remain in achieving even higher brightness and perfect indistinguishability of the entangled photons, this research marks a significant leap forward. It demonstrates the potential of quantum dots as a reliable source for building the future of quantum communication networks.

Computers benefit greatly from being connected to the internet, so we might ask: What good is a quantum computer without a quantum internet?

The secret to our modern internet is the ability for data to remain intact while traveling over long distances, and the best way to achieve that is by using photons.

Photons are single units ("quanta") of light. Unlike other quantum particles, photons interact very weakly with their environment. That stability also makes them extremely appealing for carrying quantum information over long distances,

a process that requires maintaining a delicate state of entanglement for an extended period of time. Such photons can be generated in a variety of ways.

One possible method involves using atomic-scale imperfections (quantum defects) in crystals to generate single photons in a well-defined quantum state.

Decades of optimization have resulted in fiber-optic cables that can transmit photons with extremely low loss. However, this low-loss transmission works only for light in a narrow range of wavelengths, known as the "telecom wavelength band."

Identifying quantum defects that produce photons at these wavelengths has proven difficult. Researchers at the UC Santa Barbara College of Engineering conducted research to understand why that is and describe their findings in "Rational Design of Efficient Defect-Based Quantum Emitters," published in the journal *APL Photonics*.

"Atoms are constantly vibrating, and those vibrations can drain energy from a light emitter," says UCSB materials professor Chris Van de Walle. "As a result, rather than emitting a photon, a defect might instead cause the atoms to vibrate, reducing the light-emission efficiency."

Van de Walle's group developed theoretical models to capture the role of atomic vibrations in the photon-emission process and studied the role of various defect properties in determining the degree of efficiency.

Their work explains why the efficiency of single-photon emission drastically decreases when the emission wavelength increases beyond the wavelengths of visible light (violet to red) to the infrared wavelengths in the telecom band. The model also allows the researchers to identify techniques for engineering emitters that are brighter and more efficient.

"Choosing the host material carefully, and conducting atomic-level engineering of the vibrational properties are two promising ways to overcome low efficiency," said Mark Turiansky, a postdoctoral researcher in the Van de Walle lab, a fellow at the NSF UC Santa Barbara Quantum Foundry, and the lead researcher on the project.

Another solution involves coupling to a photonic cavity, an approach that benefited from the expertise of two other Quantum Foundry affiliates: computer engineering professor Galan Moody and Kamyar Parto, a graduate student in the Moody lab.

The team hopes that their model and the insights it provides will prove useful in designing novel quantum emitters that will power the quantum networks of the future.

A new quantum computer has shattered the world record set by Google's Sycamore machine. The new 56-qubit H2-1 computer smashed 'quantum supremacy' record by 100-fold.

Between January and June 2024, Quantinuum, a computing company, ran multiple experiments on its new 56-qubit H2-1 computer to benchmark the machine's performance levels and the quality of the qubits used.

"We are entirely focused on the path to universal fault tolerant quantum computers," said Ilyas Khan, Chief Product Officer.

"This objective has not changed, but what has changed in the past few months is clear evidence of the advances that have been made possible due to the work and the investment that has been made over many, many years."

Error correction performance threshold

The company maintained that with its long-time partner Microsoft, we hit an error correction performance threshold that many believed was still years away.

The System Model H2 became the first – and only – quantum computer in the world capable of creating and computing with highly reliable logical (error corrected) qubits, according to Quantinuum.

The collaboration tackled a well-known algorithm, Random Circuit Sampling (RCS), and measured the quality of our results with a suite of tests including the

linear cross entropy benchmark (XEB) – an approach first made famous by Google in 2019 in a bid to demonstrate "quantum supremacy".

Results on H2-1 are excellent

An XEB score close to 0 says your results are noisy – and do not utilize the full potential of quantum computing. In contrast, the closer an XEB score is to 1, the more your results demonstrate the power of quantum computing. The results on H2-1 are excellent, revealing, and worth exploring in a little detail, said the company.

"Results show that whilst the full benefits of fault tolerant quantum computers have not changed in nature, they may be reachable earlier than was originally expected," added Khan.

He explained that there will be tangible benefits to our customers in their day-to-day operations as quantum computers start to perform in ways that are not classically simulatable.

"We have an exciting few months ahead of us as we unveil some of the applications that will start to matter in this context with our partners across a number of sectors."

Able to run circuits on all 56 qubits in H2-1

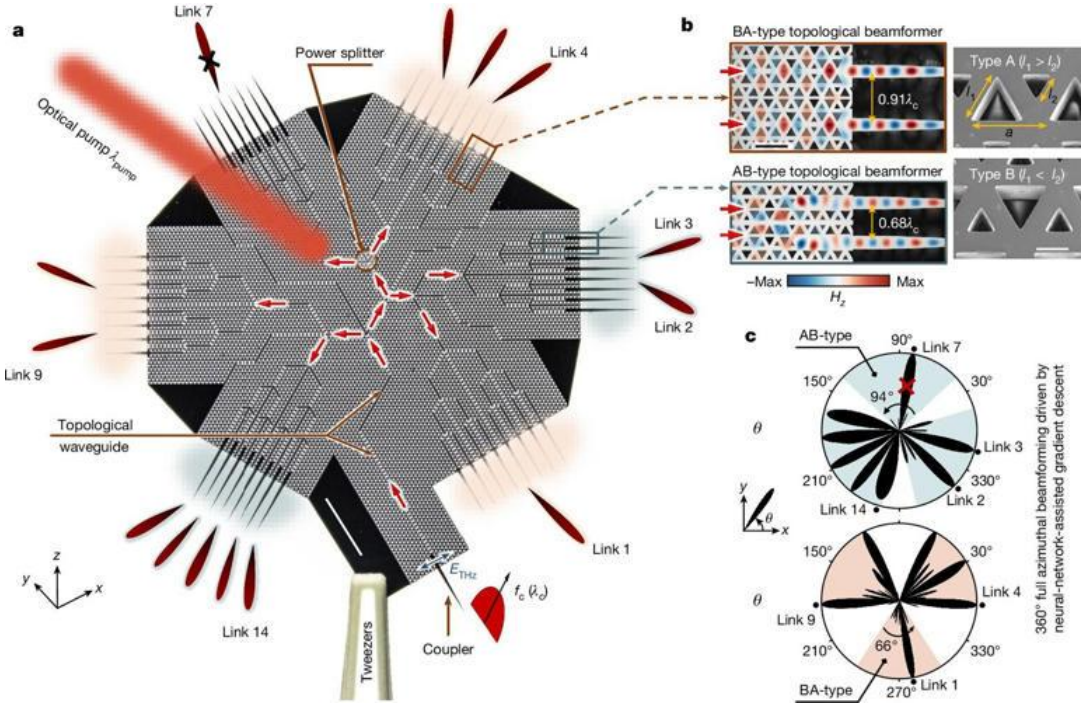
In 2019, Google's Sycamore quantum computer registered an XEB result of approximately 0.002 with the 53 superconducting qubits built into Sycamore. It was demonstrated Sycamore can complete a calculation in 200 seconds that would have taken the most powerful supercomputer at the time 10,000 years to finish.

But in the new study, Quantinuum scientists achieved an XEB score of approximately 0.35. This means the H2 quantum computer can produce results without producing an error 35% of the time, reported Live Science.

Quantinuum maintained that they have been able to run circuits on all 56 qubits in H2-1 that are deep enough to challenge high-fidelity classical simulation while achieving an estimated XEB score of ~0.35.

This >100x improvement implies the following: even for circuits large and complex enough to frustrate all known classical simulation methods, the H2 quantum computer produces results without making even a single error about 35% of the time.

In contrast to past announcements associated with XEB experiments, 35% is a significant step towards the idealized 100% fidelity limit in which the computational advantage of quantum computers is clearly in sight.



Multi-link THz topological beamformer silicon chip for 6G to XG wireless. Credit: Nature (2024). DOI: 10.1038/s41586-024-07759-5

Imagine a future where internet connections are not only lightning-fast but also remarkably reliable, even in crowded spaces. This vision is rapidly approaching reality, thanks to new research on terahertz communications

technologies. These innovations are set to transform wireless communication, particularly as communications technology advances toward the next generation of networks, 6G.

I'm an engineer who focuses on photonics, the study of how light and other electromagnetic waves are generated and detected. In this research, my colleagues and I have developed a silicon topological beamformer chip. The paper is published in the journal *Nature*. Topological

Terahertz frequencies are crucial for 6G, which telecommunications companies plan to roll out around 2030. The radio frequency spectrum used by current wireless networks is becoming increasingly congested. Terahertz waves offer a solution by using the relatively unoccupied portion of the electromagnetic spectrum between microwaves and infrared. These higher frequencies can carry massive amounts of data, making them ideal for the data-intensive applications of the future.

Our chip takes a terahertz signal from a single source and splits it into 54 smaller signals, which are then guided through 184 tiny channels with 134 sharp turns. Each beam can transmit and receive data at speeds of 40 to 72 gigabits per second, many times faster than today's 5G networks.

With the help of artificial intelligence, we designed the chip to have a specific microscopic honeycomb pattern to form lanes for the terahertz waves. The array of channels sends out powerful, focused beams that cover the entire 360 degrees around the chip. This allows a phone or other wireless device anywhere around a Wi-Fi router or other communications device using the chip to receive the high-speed signal. We demonstrated the chip by splitting an input signal of a streaming HD video into four output beams.

Beamformers in wireless networks

Terahertz waves have a shorter range compared with lower-frequency signals used in 4G and 5G networks. Terahertz beamformers address this challenge by precisely directing high-frequency signals to ensure they reach their destination without loss or degradation.

Beamformers are essential for the next generation of wireless communication. Unlike traditional antennas that broadcast signals indiscriminately, beamformers focus signals in specific directions, boosting both efficiency and reliability. Our chip ensures that those beams provide coverage in all directions.

This focused approach not only extends the signal's range but also improves its quality, even over long distances. Beamformers are likely to be crucial in managing stable connections by reducing interference as the world adds billions of connected devices.

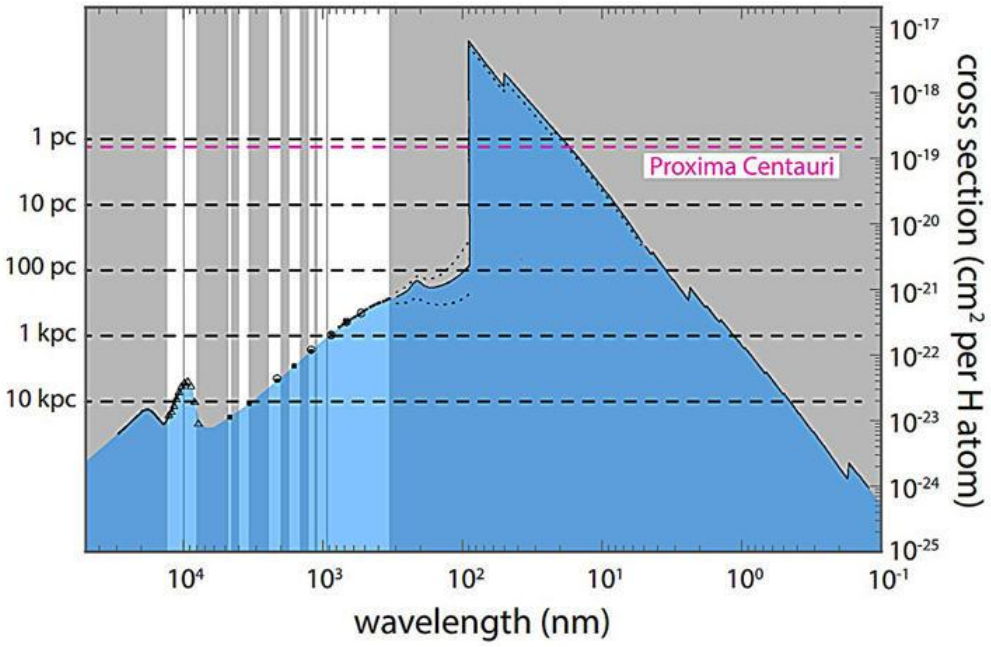
A future with terahertz beamforming

The potential impact of terahertz beamforming chips on everyday life is profound. For example, these chips could make it possible to download a 4K ultrahigh-definition movie in mere seconds compared with 11 minutes over today's W-Fi, or support immersive virtual and augmented reality experiences without any lag.

Beyond entertainment, they could make real-time holographic communication a reality, where people appear as lifelike holograms. Smart cities could use this technology to seamlessly coordinate traffic systems and emergency responses, while health care could benefit from remote surgeries where doctors control robotic instruments from afar.

The terahertz beamforming chip represents a significant step forward on the path to faster, more reliable wireless communication by overcoming the challenges of high-frequency signal transmission.

More information: Wenhao Wang et al, On-chip topological beamformer for multi-link terahertz 6G to XG wireless, *Nature* (2024). DOI: 10.1038/s41586-024-07759-5



The allowable wavelengths for interstellar quantum communications. For a given distance away (left vertical axis), quantum communications are impossible where the horizontal distance line passes through the blue region of wavelength. Gray regions are off limits for ground-based telescopes. Credit: arXiv (2024). DOI: 10.48550/arxiv.2408.02445

Thus far, the search for extraterrestrial intelligence (SETI) has used strategies based on classical science—listening for radio waves, telescopes watching for optical signals, telescopes in orbit scouring light from the atmospheres of exoplanets, scanning for laser light that might come from aliens. Could a quantum mechanical approach do better?

Latham Boyle says maybe. "It's interesting that our galaxy (and the sea of cosmic background radiation in which it's embedded) 'does' permit interstellar quantum communication in certain frequency bands," he says.

A researcher at the Higgs Center for Theoretical Physics at the University of Edinburgh in Scotland, Boyle has investigated the possibility and says, "But whereas our current telescopes are big enough to allow interstellar 'classical' communication, interstellar 'quantum' communication requires huge telescopes—much bigger than anything we've built so far."

Further, his analysis leads to another potential solution to the Fermi paradox.

For interstellar communication, Boyle wrote "it is natural to ask whether it is also possible to send or receive interstellar quantum communications." His preprint was released on the *arXiv* preprint server and has been submitted to a peer-reviewed journal.

The idea is to use entangled qubit pairs, one kept by the sender and the other sent to Earth. A few years ago it was discovered that two quantum particles could retain a quantum coherence over interstellar and even galactic distances, even entangled with one another—somehow linked so that determining a property of one entangled qubit immediately determines that of the other.

This strange connection has already been demonstrated between photons over a thousand kilometers apart, with one on Earth's surface and the other in a spacecraft orbiting the planet.

A qubit is a unit of quantum information. Quantum mechanics allows, via quantum superposition, for a particle like a photon to be in two states at once, for example, spin up and spin down. Whereas in classical communication, a photon is in a single state, a bit, that is, either spin up or spin down, but not both at the same time. The qubit's difference makes them more powerful for many applications.

Boyle concentrated on the physical requirements and limitations of sending and detecting such a qubit signal, beginning with the "quantum capacity" of a transmission—the maximum rate at which a quantum communications channel can transmit quantum information.

Much is already known about quantum communications channels from studies and experiments of quantum teleportation, quantum cryptography, quantum entanglement and other quantum phenomena. Protocols based on quantum communication are exponentially faster than those based on classical communication—channels passing one bit at a time from transmitter to receiver—for some tasks.

Using known constraints on the quantum capacity for so-called quantum erasure channels, and properties of the interstellar medium, Boyle was able to obtain two important results: a quantum capacity greater than zero requires the exchanged

photons lie within certain allowed frequency bands, and that the effective diameter of both the sending and receiving telescopes must be greater than a value which is proportional to the square root of the photon's wavelength multiplied by the distance between the telescopes.

According to Boyle's analysis, a quantum capacity that doesn't vanish requires the exchanged photons to have a wavelength less than 26.5 cm, mostly to avoid complications with the cosmic microwave background.

Moreover, while classical communications can happen if the receiver receives only a tiny percentage of the photons transmitted (as with radio signals), quantum communications requires that a majority of the photons sent be detected in the receiver's telescope.

For a ground-based telescope, that diameter would be enormous. The photon's wavelength must be at least 320 nm to get through Earth's atmosphere, and given that the distance to our nearest star, Proxima Centauri, is 4.25 light-years, Boyle finds a ground-based telescope would need to be at least 100 kilometers in diameter.

Needless to say, that's a vast difference from the largest ground-based telescope now under construction, the European Extremely Large Telescope under construction in Chile, which will have a diameter of 0.04 km (40 meters).

"In fact," Boyle said, "the required telescopes are so large that if the extraterrestrial sender has a big enough transmitting telescope, they can necessarily also see that we have not yet built a sufficiently large receiving telescope, so they would know that it doesn't yet make sense to communicate with us."

And that's maybe we haven't heard from them, he notes. "In other words, the assumption that extraterrestrials communicate quantum mechanically seems sufficient to explain the Fermi paradox."

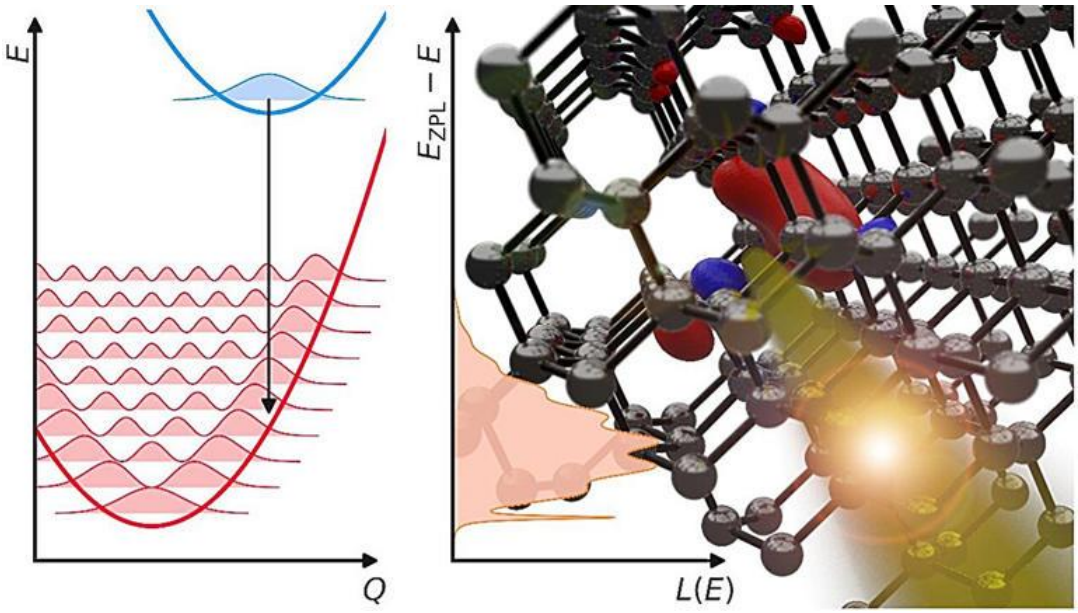
Above the atmosphere, shorter wavelengths could be utilized that would require a smaller telescope, perhaps on the moon or at Earth's L2 Lagrange Point, but even gamma rays with wavelengths of order 0.001 nm would still require telescope diameters of about 200 meters.

The telescope need not be a single dish—it could be many small dishes packed close together (either on earth or in space), but they would have to close together, "like the cells in a honeycomb," Boyle said.

A series of relays or quantum repeaters could also be placed on the line between the sender and the target, but for diameters less than 100 meters the repeater telescopes would need to be placed every tenth of an astronomical unit, which includes inside our own solar system. Keeping them in alignment might be a problem (for them at first, not us).

A missing piece is how the receiver would know that an arriving signal is quantum mechanical instead of classical, "viz." part of an entangled pair, if aliens and humans start off with no prior communication. "I think that answer is at least one additional paper in its own right," Boyle said.

More information: Latham Boyle, On Interstellar Quantum Communication and the Fermi Paradox, *arXiv* (2024). DOI: 10.48550/arxiv.2408.02445



Concept illustration depicting a quantum defect emitting a single photon. Credit: Mark Turianksy© Provided by Phys.org

Computers benefit greatly from being connected to the internet, so we might ask: What good is a quantum computer without a quantum internet?

The secret to our modern internet is the ability for data to remain intact while traveling over long distances, and the best way to achieve that is by using photons.

Photons are single units ("quanta") of light. Unlike other quantum particles, photons interact very weakly with their environment. That stability also makes them extremely appealing for carrying quantum information over long distances, a process that requires maintaining a delicate state of entanglement for an extended period of time. Such photons can be generated in a variety of ways.

One possible method involves using atomic-scale imperfections (quantum defects) in crystals to generate single photons in a well-defined quantum state.

Decades of optimization have resulted in fiber-optic cables that can transmit photons with extremely low loss. However, this low-loss transmission works only for light in a narrow range of wavelengths, known as the "telecom wavelength band."

Identifying quantum defects that produce photons at these wavelengths has proven difficult. Researchers at the UC Santa Barbara College of Engineering conducted research to understand why that is and describe their findings in "Rational Design of Efficient Defect-Based Quantum Emitters," published in the journal *APL Photonics*.

"Atoms are constantly vibrating, and those vibrations can drain energy from a light emitter," says UCSB materials professor Chris Van de Walle. "As a result, rather than emitting a photon, a defect might instead cause the atoms to vibrate, reducing the light-emission efficiency."

Van de Walle's group developed theoretical models to capture the role of atomic vibrations in the photon-emission process and studied the role of various defect properties in determining the degree of efficiency.

Their work explains why the efficiency of single-photon emission drastically decreases when the emission wavelength increases beyond the wavelengths of visible light (violet to red) to the infrared wavelengths in the telecom band. The model also allows the researchers to identify techniques for engineering emitters that are brighter and more efficient.

"Choosing the host material carefully, and conducting atomic-level engineering of the vibrational properties are two promising ways to overcome low efficiency," said Mark Turiansky, a postdoctoral researcher in the Van de Walle lab, a fellow at the NSF UC Santa Barbara Quantum Foundry, and the lead researcher on the project.

Another solution involves coupling to a photonic cavity, an approach that benefited from the expertise of two other Quantum Foundry affiliates: computer engineering professor Galan Moody and Kamyar Parto, a graduate student in the Moody lab.

The team hopes that their model and the insights it provides will prove useful in designing novel quantum emitters that will power the quantum networks of the future.

More information: Mark E. Turiansky et al, Rational design of efficient defect-based quantum emitters, *APL Photonics* (2024). DOI: 10.1063/5.0203366

Provided by University of California - Santa Barbara

How an old short story may predict the chaotic collapse of the open internet

How will the internet evolve in the coming decades? Fiction writers have explored some possibilities.

In his 2019 novel "Fall," science fiction author Neal Stephenson imagined a near future in which the internet still exists. But it has become so polluted with misinformation, disinformation and advertising that it is largely unusable.

Characters in Stephenson's novel deal with this problem by subscribing to "edit streams" – human-selected news and information that can be considered trustworthy.

The drawback is that only the wealthy can afford such bespoke services, leaving most of humanity to consume low-quality, noncurated online content.

To some extent, this has already happened: Many news organizations, such as The New York Times and The Wall Street Journal, have placed their curated content behind paywalls. Meanwhile, misinformation festers on social media platforms like X and TikTok.

Stephenson's record as a prognosticator has been impressive – he anticipated the metaverse in his 1992 novel "Snow Crash," and a key plot element of his "Diamond Age," released in 1995, is an interactive primer that functions much like a chatbot.

On the surface, chatbots seem to provide a solution to the misinformation epidemic. By dispensing factual content, chatbots could supply alternative sources of high-quality information that aren't cordoned off by paywalls.

Ironically, however, the output of these chatbots may represent the greatest danger to the future of the web – one that was hinted at decades earlier by Argentine writer Jorge Luis Borges.

The rise of the chatbots

Today, a significant fraction of the internet still consists of factual and ostensibly truthful content, such as articles and books that have been peer-reviewed, fact-checked or vetted in some way.

The developers of large language models, or LLMs – the engines that power bots like ChatGPT, Copilot and Gemini – have taken advantage of this resource.

To perform their magic, however, these models must ingest immense quantities of high-quality text for training purposes. A vast amount of verbiage has already been scraped from online sources and fed to the fledgling LLMs.

The problem is that the web, enormous as it is, is a finite resource. High-quality text that hasn't already been strip-mined is becoming scarce, leading to what The New York Times called an "emerging crisis in content."

This has forced companies like OpenAI to enter into agreements with publishers to obtain even more raw material for their ravenous bots. But according to one prediction, a shortage of additional high-quality training data may strike as early as 2026.

As the output of chatbots ends up online, these second-generation texts – complete with made-up information called "hallucinations," as well as outright errors, such as suggestions to put glue on your pizza – will further pollute the web.

And if a chatbot hangs out with the wrong sort of people online, it can pick up their repellent views. Microsoft discovered this the hard way in 2016, when it had to pull the plug on Tay, a bot that started repeating racist and sexist content.

Over time, all of these issues could make online content even less trustworthy and less useful than it is today. In addition, LLMs that are fed a diet of low-calorie content may produce even more problematic output that also ends up on the web.

An infinite – and useless – library

It's not hard to imagine a feedback loop that results in a continuous process of degradation as the bots feed on their own imperfect output.

A July 2024 paper published in Nature explored the consequences of training AI models on recursively generated data. It showed that "irreversible defects" can lead to "model collapse" for systems trained in this way – much like an image's copy and a copy of that copy, and a copy of that copy, will lose fidelity to the original image.

How bad might this get?

Consider Borges' 1941 short story "The Library of Babel." Fifty years before computer scientist Tim Berners-Lee created the architecture for the web, Borges had already imagined an analog equivalent.

In his 3,000-word story, the writer imagines a world consisting of an enormous and possibly infinite number of hexagonal rooms. The bookshelves in each room hold uniform volumes that must, its inhabitants intuit, contain every possible permutation of letters in their alphabet.

Initially, this realization sparks joy: By definition, there must exist books that detail the future of humanity and the meaning of life.

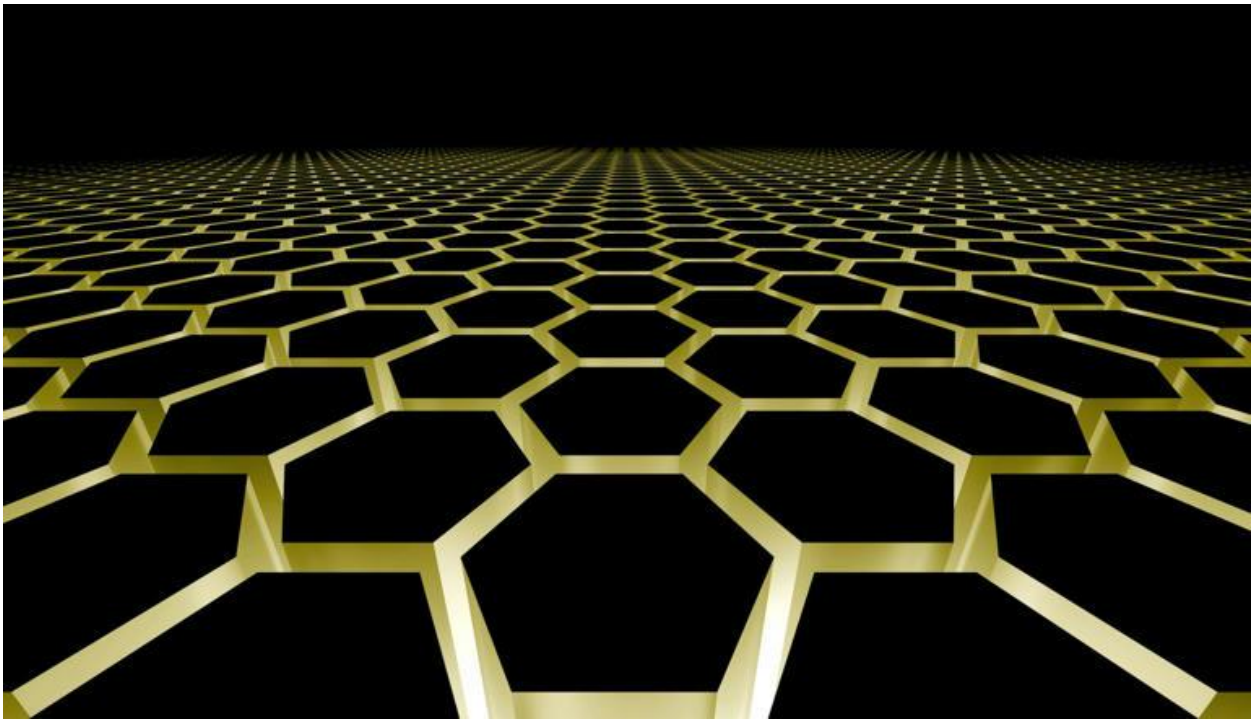
The inhabitants search for such books, only to discover that the vast majority contain nothing but meaningless combinations of letters. The truth is out there – but so is every conceivable falsehood. And all of it is embedded in an inconceivably vast amount of gibberish.

Even after centuries of searching, only a few meaningful fragments are found. And even then, there is no way to determine whether these coherent texts are truths or lies. Hope turns into despair.

Will the web become so polluted that only the wealthy can afford accurate and reliable information? Or will an infinite number of chatbots produce so much tainted verbiage that finding accurate information online becomes like searching for a needle in a haystack?

The internet is often described as one of humanity's great achievements. But like any other resource, it's important to give serious thought to how it is maintained and managed – lest we end up confronting the dystopian vision imagined by Borges.

Roger J. Kreuz, Associate Dean and Professor of Psychology, *University of Memphis*



Quantum Teleportation Achieved Over Internet For First Time

A quantum state of light has been successfully teleported through more than 30 kilometers (around 18 miles) of fiber optic cable amid a torrent of internet traffic – a feat of engineering once considered impossible.

The impressive demonstration by researchers in the US may not help you beam to work to beat the morning traffic, or download your favourite cat videos faster.

However, the ability to teleport quantum states through existing infrastructure represents a monumental step towards achieving a quantum-connected computing network, enhanced encryption, or powerful new methods of sensing.

"This is incredibly exciting because nobody thought it was possible," says Prem Kumar, a Northwestern University computing engineer who led the study.

"Our work shows a path towards next-generation quantum and classical networks sharing a unified fiber optic infrastructure. Basically, it opens the door to pushing quantum communications to the next level."

Bearing a passing resemblance to Star Trek transport systems that ghost passengers across time and space in the blink of an eye, teleportation takes the quantum possibilities of an object in one location and, by carefully destroying it, forces the same balance of possibilities onto a similar object in another location.

Though acts of measuring the two objects seal their fates in the same instant, the process of entangling their quantum identities still requires sending a single wave of information between points in space.

Like fairy floss in a spring shower, the quantum state of any object is a hazy smear of possibility at risk of melting into reality moments after creation. Electromagnetic waves of radiation and the thermal bumping-and-grinding of moving particles quickly reduces the quantum significance into decoherence if it isn't protected in some way.

Shielding quantum states inside computers is one thing. Sending a single photon through optical fibers humming with bank transactions, cat videos, and text messages while protecting its quantum state is far more daunting. You might as well cast your quantum fairy floss into the Mississippi and hope it tastes as good at the end.

Optical fibers are used to transmit internet communication. (alphaspirit it/Canva)

To preserve their lonely photon's precious state against a 400 gigabit-per-second current of internet traffic, the team of researchers applied a variety of techniques that restricted the photon's channel and reduced the chances it might scatter and mix with other waves.

"We carefully studied how light is scattered and placed our photons at a judicial point where that scattering mechanism is minimized," says Kumar.

"We found we could perform quantum communication without interference from the classical channels that are simultaneously present."

While other research groups have successfully transmitted quantum information alongside classical data streams in simulations of the internet, Kumar's team is the first to teleport a quantum state alongside an actual internet stream.

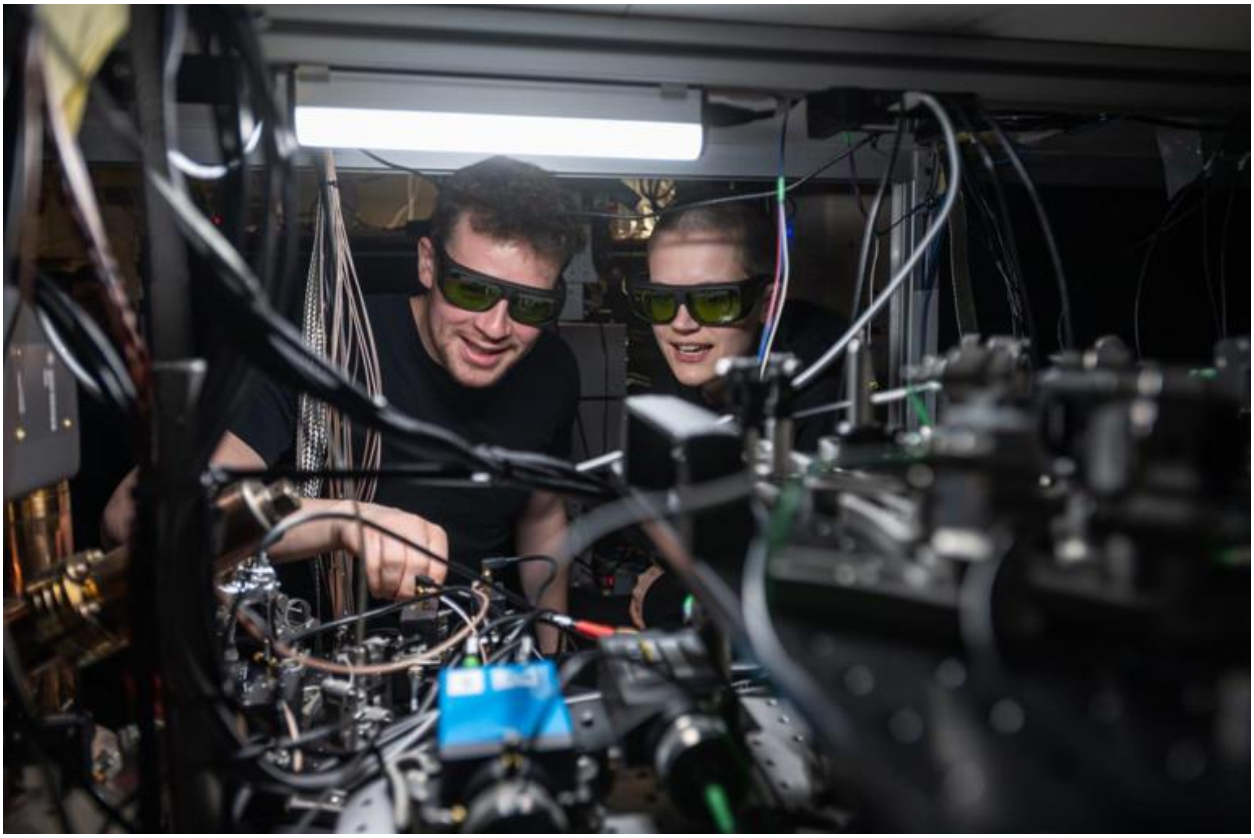
Each test further suggests the quantum internet is inevitable, giving computing engineers a whole new toolkit for measuring, monitoring, encrypting, and calculating our world like never before, without needing to reinvent the internet to do it.

"Quantum teleportation has the ability to provide quantum connectivity securely between geographically distant nodes," says Kumar.

"But many people have long assumed that nobody would build specialized infrastructure to send particles of light. If we choose the wavelengths properly, we won't have to build new infrastructure. Classical communications and quantum communications can coexist."

This research was published in *Optica*.

First-ever distributed quantum algorithm is a breakthrough for quantum supercomputers



Dougal Main and Beth Nichol working on the distributed quantum computer.(CREDIT: John Cairns)© The Brighter Side of News

Scientists have taken a major step toward building large-scale quantum computers by successfully linking two separate quantum processors into a single, fully connected system.

This breakthrough in distributed quantum computing offers a promising way to overcome the challenges of scaling up quantum computers and has the potential to revolutionize fields such as cryptography, drug discovery, and artificial intelligence.

A New Approach to Quantum Computing

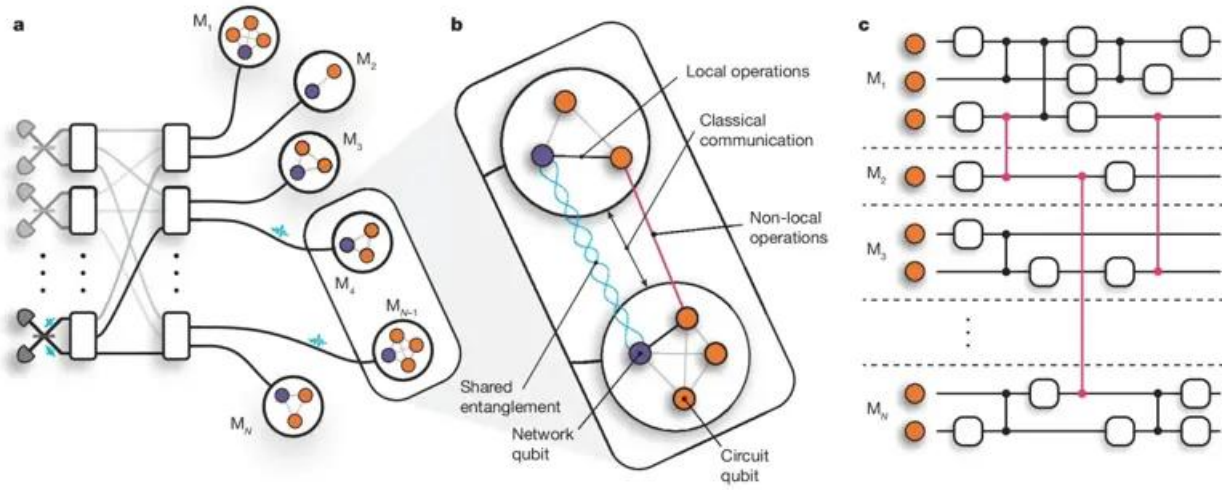
Quantum computers rely on qubits, which can exist in multiple states simultaneously due to quantum superposition. This ability allows them to process complex problems much faster than classical computers. However, increasing the number of qubits within a single system while maintaining control and connectivity is an immense challenge.

Instead of cramming more qubits into a single machine, researchers at Oxford University Physics have demonstrated a distributed approach.

They connected two separate quantum modules using photonic links—fiber-optic cables that transmit quantum information using light instead of electrical signals. This method enables qubits in different modules to interact as if they were in the same processor.

The study 'Distributed Quantum Computing across an Optical Network Link,' is published in the journal Nature.

Dougal Main, a lead researcher on the project, explains: "Previous demonstrations of quantum teleportation have focused on transferring quantum states between physically separated systems. In our study, we use quantum teleportation to create interactions between these distant systems. By carefully tailoring these interactions, we can perform logical quantum gates—the fundamental operations of quantum computing—between qubits housed in separate quantum computers."



Schematic of a DQC architecture comprising photonically interconnected modules. Entanglement is heralded between network qubits through the interference of photons on beam splitters. (CREDIT: Nature)© The Brighter Side of News

The Role of Quantum Teleportation

The key to this distributed system is quantum teleportation, a process that allows information to be transferred between qubits without direct transmission. This is achieved through quantum entanglement, where two particles remain correlated even when separated by long distances.

When one qubit in a module is entangled with another in a separate module, performing an operation on one immediately affects the other. This enables the execution of quantum gate teleportation (QGT), a method that implements logical quantum operations across a network. Unlike direct data transfer, which risks information loss due to noise or interference, teleportation ensures that the quantum state remains intact.

Professor David Lucas, lead scientist for the UK Quantum Computing and Simulation Hub, says: "Our experiment demonstrates that network-distributed quantum information processing is feasible with current technology. Scaling up quantum computers remains a formidable technical challenge that will likely require new physics insights as well as intensive engineering effort over the coming years."

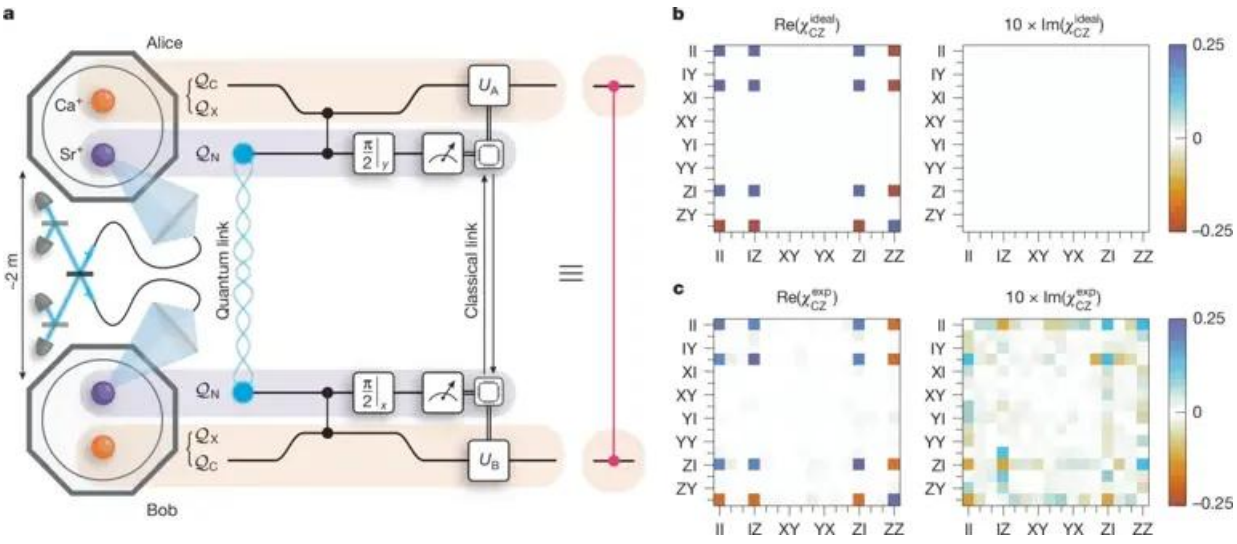
Breaking the Scalability Barrier

For quantum computers to reach their full potential, they must handle millions of qubits. Packing all those qubits into a single machine would create enormous technical challenges, from maintaining quantum coherence to managing complex interconnections. The distributed approach sidesteps these issues by linking smaller modules together.

In the Oxford experiment, the two quantum modules were separated by about two meters and contained dedicated network and circuit qubits. By generating entanglement between network qubits, researchers teleported a controlled-Z

(CZ) gate—a key quantum logic operation—between circuit qubits in separate modules with 86% fidelity.

They then successfully executed Grover's search algorithm, a quantum algorithm designed to quickly find solutions within large datasets. The method achieved a 71% success rate, demonstrating the feasibility of distributed quantum computing.



Teleportation of a CZ gate between two trapped-ion modules. (CREDIT: Nature)© The Brighter Side of News

Quantum physicist Dougal Main describes the approach as similar to how traditional supercomputers function: "These are made up of smaller computers linked together to achieve capabilities that are greater than those of each separate unit.

This strategy circumvents many of the engineering obstacles associated with packing ever larger numbers of qubits into a single device, while preserving the delicate quantum properties needed for accurate and robust computations."

Toward a Quantum Internet

The success of this experiment suggests that quantum processors could eventually be networked across vast distances, forming a "quantum internet." This could enable ultra-secure communication, large-scale computational collaboration, and advances in quantum sensing.

Unlike traditional networks, where data is transmitted through classical signals, a quantum internet would rely on entanglement to instantly share information across different nodes. This could revolutionize industries requiring high levels of security, such as finance and national defense.

Additionally, the modular approach allows for system upgrades without disrupting the overall network. "By interconnecting the modules using photonic links, the system gains valuable flexibility, allowing modules to be upgraded or swapped out without disrupting the entire architecture," says Main.

With ongoing advancements in quantum computing and networking, this breakthrough provides a crucial foundation for future scalable quantum systems. While many engineering challenges remain, the success of distributed quantum computing brings researchers one step closer to harnessing the full power of quantum mechanics.

What Is The Internet Of Bodies? And How Is It Changing Our World?

Have you heard the term the Internet of Bodies (IoB)? That may conjure up a few thoughts that have nothing to do with the true nature of the term, but it's about using the human body as the latest data platform. At first, this concept seems quite creepy, but then when you realize the possibilities it creates, it becomes quite exciting. Here we explore what the Internet of Bodies is, some examples in use today, and a few of the challenges it presents.

What Is The Internet Of Bodies? And How Is It Changing Our World?

What is the Internet of Bodies (IoB)?

When the Internet of Things (IoT) connects with your body, the result is the Internet of Bodies (IoB). The Internet of Bodies (IoB) is an extension of the IoT and basically connects the human body to a network through devices that are ingested, implanted, or connected to the body in some way. Once connected, data can be exchanged, and the body and device can be remotely monitored and controlled.

There are three generations of Internet of Bodies that include:

· Body external: These are wearable devices such as Apple Watches or Fitbits that can monitor our health.

· Body internal: These include pacemakers, cochlear implants, and digital pills that go inside our bodies to monitor or control various aspects of our health.

· Body embedded: The third generation of the Internet of Bodies is embedded technology where technology and the human body are melded together and have a real-time connection to a remote machine.

Progress in wireless connectivity, materials, and tech innovation is allowing implantable medical devices (IMD) to scale and be viable in many applications.

Examples of Internet of Bodies Devices in Use or Development

The most recognized example of Internet of Bodies is a defibrillator or pacemaker, a small device placed in the abdomen or chest to help patients with heart conditions control abnormal heart rhythms with electrical impulses. In 2013, former United States Vice President Dick Cheney got his WiFi-connected defibrillator replaced with one without WiFi capacity. It was feared that he could be assassinated by electric shock if a rogue agent hacked the device.

A "smart pill" is another IoB device. These pills have edible electronic sensors and computer chips in them. Once swallowed, these digital pills can collect data from our organs and then send it to a remote device connected to the internet. The first digital chemotherapy pill is now in use that combines chemotherapy drugs with a sensor that captures, records, and shares information with healthcare providers (with the patient's consent) regarding the drug dosage and time, plus other data on rest and activity, heart rate and more.

"Smart contact lenses" are being developed that integrate sensors and chips that can monitor health diagnostics based on information from the eye and eye fluid. One smart contact lens in development aims to monitor glucose levels that will hopefully allow diabetics to monitor their glucose levels without repeated pinpricks throughout the day.

Taking it up a notch is the Brain Computer Interface (BCI), where a person's brain is actually merged with an external device for monitoring and controlling in real-time. The ultimate goal is to help restore function to

individuals with disabilities by using brain signals rather than conventional neuromuscular pathways.

But not all Internet of Bodies use cases are for healthcare reasons. Bioengineering company, Biohax has embedded chips in more than 4,000 people primarily for convenience. In one widely reported example, 50 employees of Three Square Market agreed to have an RFID microchip the size of a large grain of rice (similar to what's embedded in pets to be able to identify and locate them when they are lost) implanted. This chip allows these employees to gain access to the building without a key, pay for items with a wave of their hand at the vending machine by deducting the amount immediately from their account rather than use money and log onto their computers.

Challenges Faced by Internet of Bodies Technology

The situation of U.S. Vice President Cheney getting a defibrillator not connected to WiFi for security reasons illustrates one of the biggest challenges faced by Internet of Bodies technology—how to secure the devices and information they collect and transmit. Nearly half a million pacemakers were recalled in 2017 by the U.S. Food and Drug Administration over security issues requiring a firmware update. The security challenges faced by Internet of Bodies tech are similar to what plagues Internet of Things generally, but there can be life and death consequences when IoB devices are involved. Additionally, IoB devices create another cyber security challenge that will need to be safeguarded from hackers.

Privacy is also of paramount concern. Questions about who can access the data and for what purpose need answers. For example, a device that monitors health diagnostics could also track unhealthy behaviors. Will health insurance

companies be able to deny coverage when a customer's IoB device reports their behavior? A cochlear implant could restore hearing, but it might also record all audio in a person's environment. Will that data remain private?

As Internet of Bodies tech continues to grow, regulatory and legal issues will have to be resolved and policies built around the proper use of the technology.

The Internet of Bodies Will Change Everything, for Better or Worse

Oct 29, 2020

Illustration by Alyson Youngblood/RAND Corporation

The rise of devices that connect the human body to the web is accelerating rapidly. This Internet of Bodies could revolutionize health care and improve our quality of life. But without appropriate guardrails,

it could also jeopardize our most intimate personal information and introduce several ethical concerns.
Ross Compton was there when a fire ravaged his $400,000 home in Middletown, Ohio, in September 2016. Fortunately, Compton told investigators, he was able to stuff a few bags with several possessions—including the charger for an external heart pump he needed to survive—before shattering a window with his cane and escaping.

But as the smoke cleared, police began to suspect that Compton's story was a fabrication.

His statements were inconsistent. The rubble smelled of gasoline. And it seemed implausible that someone fleeing a burning house—especially someone with a medical condition like Compton's—could execute such a complex escape plan.

Eventually, investigators were able to indict Compton on felony charges of aggravated arson and insurance fraud. Their star witness? His pacemaker.

Police obtained a warrant to retrieve data on Compton's heart activity before, during, and after the fire. After reviewing this information, a cardiologist concluded that it was “highly improbable” Compton would've been able to escape the flames so quickly, while lugging so many belongings.

Compton pleaded not guilty. His attorney argued that the pacemaker data should be thrown out; including it would violate doctor-patient privilege and Compton's constitutional right to privacy, the lawyer said.

The case was strange, arguably sad, and fraught with difficult questions. Regardless of whether Compton really torched his house, should a life-saving device inside someone's body be part of a case that might put them behind bars?

We may not know the answer for some time. Compton passed away in July at the age of 62, leaving his case—and whatever precedent it might have set—unresolved.

This may seem like a one-of-a-kind chain of events, an aberration. But as industries usher in a new era of devices that track personal information by leveraging the internet and the human body in equal measure, it won't be the last.

When it comes to regulating the Internet of Bodies, it's the Wild West.

Share on Twitter
This type of technology, appropriately dubbed the Internet of Bodies (IoB), has the potential to improve our lives in countless ways. But the risks are just as legion. A new RAND study explores the Internet of Bodies, identifying implications for policy that could help maximize the IoB's upside while mitigating these risks.

“When it comes to regulating IoB, it's the Wild West,” said Mary Lee, a mathematician at RAND and lead author of the study.

“There are many benefits to these technologies that some consider too great to be slowed down by policy. But we need to have a larger discussion about what those benefits will cost us—and how we might avoid some of the risk altogether.”

What Is the Internet of Bodies?

Internet-connected devices like smart thermostats, voice-activated assistants, and web-enabled refrigerators have become ubiquitous in American homes. These technologies are part of the Internet of Things (IoT), which has flourished in recent years as consumers and businesses flock to smart devices for convenience, efficiency, and, in many cases, fun.

Internet of Bodies technologies fall under the broader IoT umbrella. But as the name suggests, IoB devices introduce an even more

intimate interplay between humans and gadgets. IoB devices monitor the human body, collect health metrics and other personal information, and transmit those data over the internet. Many devices, such as fitness trackers, are already in use.

The Internet of Bodies: Opportunities, Risks, and Governance

Torrents of data on everything from diets to social interactions could help improve preventative health care, increase employee productivity, and encourage people to become active participants in their health.

Artificial pancreases could automate insulin dosing for diabetics. Brain-computer interfaces could allow amputees to control prosthetic limbs with their minds. And smart diapers could alert parents via Bluetooth app when their baby needs to be changed.

But despite its potential to revolutionize just about everything in ways that could be helpful, the Internet of Bodies could jeopardize our most intimate personal information.

“There are vast amounts of data being collected, and the regulations about that data are really murky,” Lee said. “There's not a lot of clarity about who owns the data, how it's being used, and even who it can be sold to.”

Lee and her colleagues examined the risks that IoB devices could pose across three areas: data privacy, cybersecurity, and ethics. The team also identified recommendations that could help policymakers balance the IoB's many risks and rewards.

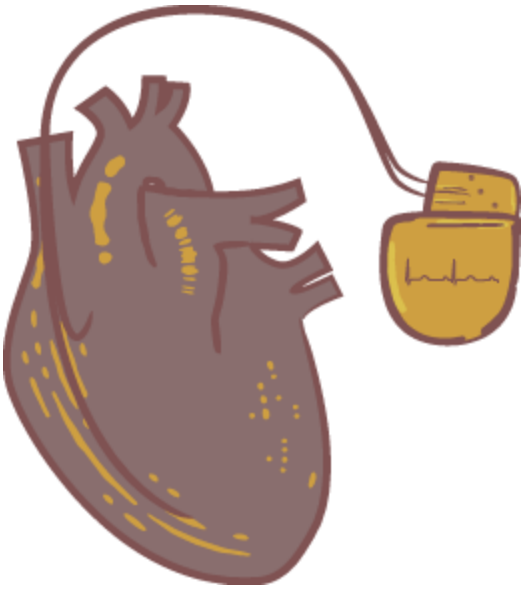
IoB Privacy Risks

IoB devices already in use and those in development can track, record, and store users' whereabouts, bodily functions, and what they see, hear, and even think. According to the RAND researchers, there are many unresolved questions about who has the authority to access these data—and how they can use it.

The data collection process can pose an inherent risk to privacy, depending on what's being collected, how often, whether users provided informed consent beforehand, and whether they can easily opt out of collection or forbid companies to sell their data.

“There's a patchwork of regulations in the U.S. that makes it unclear how safe it is to use these devices,” Lee said. “There is no national regulation on data brokers, so, depending on which state you live in, data brokers may be able to sell your information to third parties, who can then build a profile on you based on that sold data.”

Implantable Cardiac Devices



Newer cardiac pacemakers and implantable cardioverter defibrillators can provide real-time and continuous information about a patient's cardiac fluctuations. These devices can also regulate heart rates in

patients whose hearts beat too fast or too slowly, and can help treat heart failure.

The benefits of implantable cardiac devices are clearly documented—they can improve a patient's quality of life and, in many cases, sustain their life. But as the case of Ross Compton illustrates, it's unclear whether law enforcement use of IoB data violates constitutional protections against self-incrimination and unreasonable search and seizure.

How they work:

The device is implanted in the chest, with insulated wires that connect to the heart. A transmitter located in the patient's home wirelessly transfers the recorded data to their physician.

Additional risks:

Internet connectivity introduces the potential for these devices to be hacked and the data they transmit to be compromised.

Productivity Technology

Amazon has patented technologies for a wristband designed to track and record workers' locations and hand movements. If the wristband senses a lull in productivity, then it would vibrate to nudge the employee to focus.

While it's unclear whether Amazon will ever manufacture this device, such productivity technology could help businesses become more efficient and less prone to error. But because this would give employers highly personal information about their workers, such as information about their bathroom breaks, there's concern about whether the technology described in Amazon's patents might violate employees' right to privacy.

How it works:

The wristband would send ultrasonic pulses at predetermined intervals to track hand movements and the relative positions of employees' hands and warehouse bins.

Additional risks:

Employees may view this technology as intrusive, which could harm retention.

How Policy Could Mitigate IoB Privacy Risks

- Congress should consider establishing data transparency and protection standards for data collected by IoB devices.
- Congress could draw lessons from the successes and failures of recent privacy laws established in Europe and California. Lawmakers could also consider ways to ensure that IoB users have control over their personal information, including the right to opt out of data collection.
- Federal and state governments should consider regulations for data brokers and restrictions on who can collect data, how those data are used, and whether data may be sold to third parties.
- Policymakers should consider regulations on how insurers, employers, and others are permitted to use IoB data.

IoB Security Risks

IoB devices can be prone to the same security flaws of IoT devices, or any other technology that stores information in the cloud. But, given

the nature of IoB devices and the data they collect, the stakes are particularly high. Vulnerabilities could allow unauthorized parties to leak private information, tamper with data, or lock users out of their accounts.

In the case of some implanted medical devices, hackers could potentially manipulate the devices to cause physical injury or even death. National security is also a concern, because any IoB-collected data have the potential to reveal sensitive information, such as the location of U.S. service members.

Health Trackers

IoB bracelets, watches, rings, and smartphone apps can track steps, heart rate, sleep patterns, and other physical data, such as alcohol consumption. Many devices also offer user-friendly analytics, giving individuals greater visibility into their own health. They may help users identify and seek care for potential health issues earlier on. And they encourage better preventative health measures, such as a healthy diet and exercise.

Still, the volume of personal data that these devices collect, security vulnerabilities, and the potential for user error have created a perfect storm. Companies, hackers, and even foreign adversaries can exploit user data for financial or political gain.

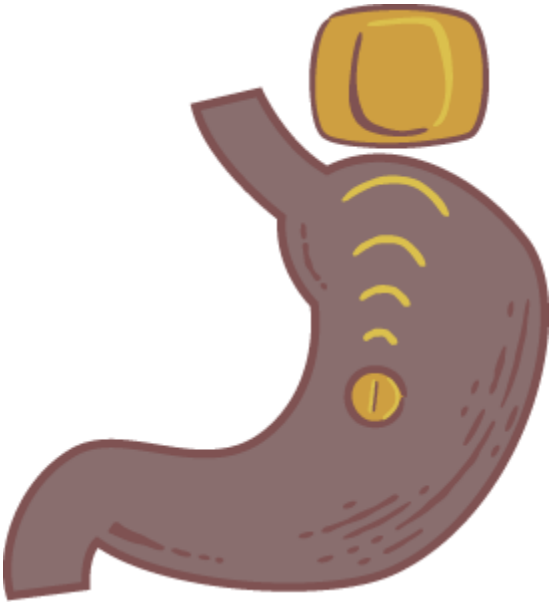
How they work:

These devices operate by using advanced accelerometers and other sensors that can translate movement into digital measurements.

Additional risks:

Some studies have shown that constant tracking of biometric activity through health apps such as sleep trackers can increase users' anxiety and worsen insomnia and other conditions.

Digital Pills



In 2017, the Food and Drug Administration (FDA) approved the first digital pill with embedded sensors that record that the medication was taken. The pill has been successful at treating schizophrenia and some forms of bipolar disorder and depression—conditions for which patients' adherence to treatment is critical to preventing relapse.

Patients can grant caregivers and physicians access to this information through a web-based portal. This can help health care providers confirm whether patients are following their treatment plans. But this comes at the cost of potentially exposing health care provider networks to cyberattacks.

How they work:

The pill's sensor sends a message to a wearable patch that transmits the information to a mobile app so that patients can track the ingestion of the medication on their smartphones.

Additional risks:

Data gathered by digital pills could introduce the potential for insurance companies to monitor whether and when a patient is taking their medication—and deny coverage for those who do not follow their prescribed regimen.

How Policy Could Mitigate IoB Security Risks

- Although the FDA has led efforts to promote cybersecurity best practices for parts of the IoB ecosystem, not all IoB devices fall within FDA oversight. Federal agencies could model an IoB-specific framework after the National Institute of Standards and Technology's cybersecurity framework.
- Existing FDA efforts could expand to include consumer health devices and electronic health records.
- Policymakers could establish cybersecurity certifications that are similar to the Energy Star label developed by the Environmental Protection Agency. This could incentivize the use of secure devices and increase consumer awareness.

IoB Ethical Concerns

Privacy and security risks are inherently ethical issues for the individuals whose data are compromised. But the IoB raises further ethical concerns, including inequity and threats to personal autonomy.

Without insurance coverage, internet access, or a certain level of tech-savviness, some groups could miss out on the IoB's immediate benefits, as well as its influence on public health initiatives in the long run. And because the IoB is in its infancy, there are still basic

questions about whether individuals have ownership over their personal data or have the right to opt out of data collection.

“There are devices parents can give to their children to help keep track of them, usually with some sort of microphone and camera,” Lee said. “So even though a parent has the right to keep an eye on their child, if the child is at school or on a playdate, other children are unknowingly being monitored as well.”

Direct-to-Consumer Genetic Testing

Genetic testing kits can provide interesting ancestry information and even personalized insights on health and disease risks. But with little oversight, these services could unknowingly create challenges for individuals' future descendants—long before they've even been conceived.

For example, results from a genetic testing kit or the use of a particular IoB medical device might identify someone as a carrier of a genetic disease that could be passed on to their children. This could one day result in those children being denied insurance coverage or other benefits.

How it works:

A consumer purchases a testing kit and provides a sample of saliva or blood via mail. A lab analyzes the sample to look for genetic variations, and the results are communicated via a web portal.

Additional risks:

Without regulation, companies that administer these kits could sell the information they gather to third parties. There's also a question about whether ancestry information generated from these tests is accurate.

Emotional Sensors

Artificial intelligence (AI) software companies are developing systems that can detect and collect data on human emotions by analyzing facial expressions, voice intonations, and other audio and visual signals.

Some argue these technologies could help reduce car accidents, show companies how consumers feel about their content, and even teach children about empathy. Although these emotional perception technologies are still very new, other facial recognition technologies have been found to be inaccurate when identifying women and minorities, which could potentially put these groups at risk of bias.

How they work:

AI uses machine learning techniques to analyze millions of videos then uses those data points to measure and analyze brow furrows, eyelash movements, nose wrinkles, and other facial reactions.

Additional risks:

The increasing complexity of gathered facial and voice recognition data raises concerns about potential surveillance and privacy violations.

How Policy Could Mitigate Ethical Concerns

- Policymakers should consider regulating the terms and conditions under which IoB technologies can be used. They should also consider protections for vulnerable groups, especially to ensure that users have rights over technologies implanted in their bodies.
- Federal agencies and foundations could fund research related to IoB data collection and health care disparities.
- As the IoB becomes more mainstream, medical providers, consumer groups, and IoB developers will need to conduct research and spread information about the realistic and pragmatic benefits, as well as the likely harms.
- The Federal Trade Commission could play a larger role to ensure that IoB marketing claims about improved well-being or specific health treatments are backed by appropriate evidence.

Project Credits

Maria Gardner (Story) and Alyson Youngblood (Design, illustration, and development)

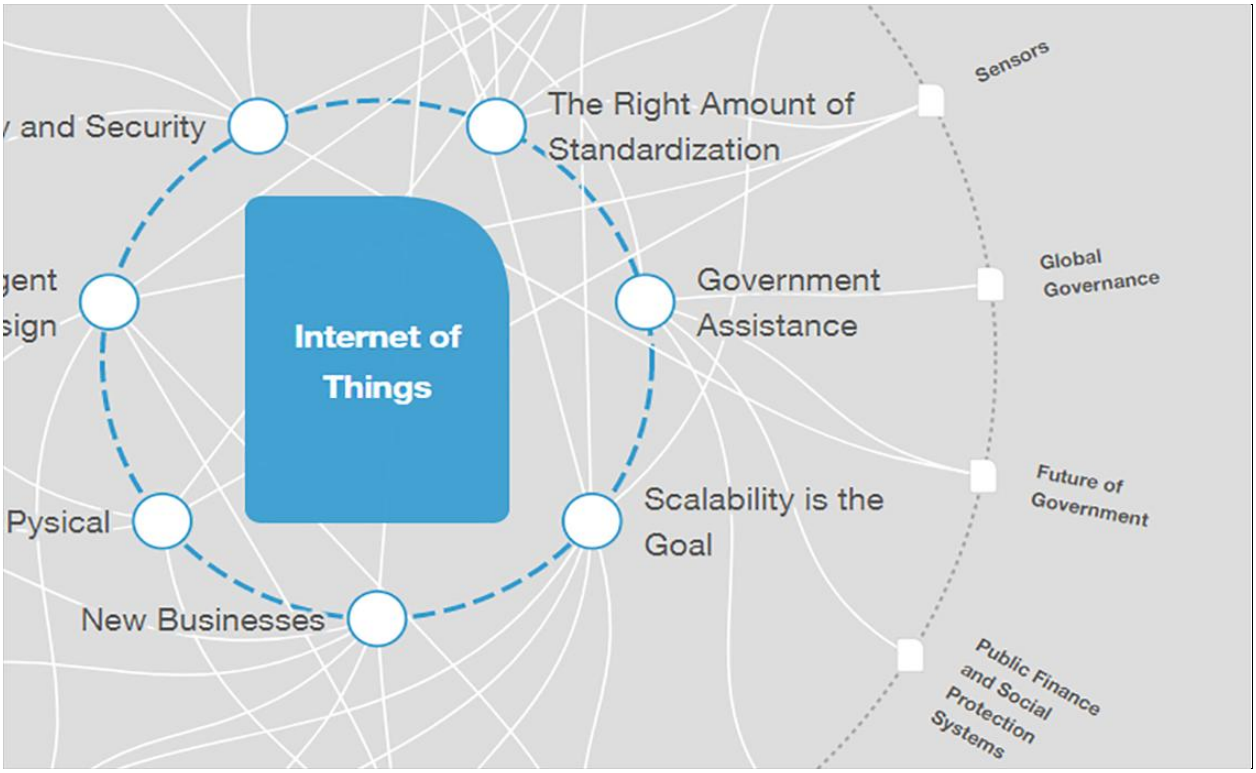
Illustration of man based on photo by PeopleImages/Getty

The research on which this article is based was conducted by RAND researchers. The full report, The Internet of Bodies: Opportunities, Risks

and Governance (by Mary Lee, Benjamin Boudreaux, Ritika Chaturvedi, Sasha Romanosky, and Bryce Downing, 2020), was peer-reviewed and published to rand.org; it is free to read online or download for personal use. Learn more about RAND copyright and permissions.

Tracking how our bodies work could change our lives

The “Internet of Bodies” connects us through fitness trackers and other devices.



THE BIG PICTURE

Explore and monitor how Internet of Things is affecting economies, industries and global issues

Internet of Things

This article is part of:Centre for Urban Transformation

- We're entering the era of the "Internet of Bodies": collecting our physical data via a range of devices that can be implanted, swallowed or worn.
- The result is a huge amount of health-related data that could improve human wellbeing around the world, and prove crucial in fighting the COVID-19 pandemic.
- But a number of risks and challenges must be addressed to realize the potential of this technology, from privacy issues to practical hurdles.

In the special wards of Shanghai's Public Health Clinical Center, nurses use smart thermometers to check the temperatures of COVID-19 patients. Each person's temperature is recorded with a sensor, reducing the risk of infection through contact, and the data is sent to an observation dashboard. An abnormal result triggers an alert to medical staff, who can then intervene promptly. The gathered data also allows medics to analyse trends over time.

The smart thermometers are designed by VivaLNK, a Silicon-Valley based startup, and are a powerful example of the many digital products and services that are revolutionizing healthcare. After the Internet of Things, which transformed the way we live, travel and work by connecting everyday objects to the Internet, it's now time for the Internet of Bodies. This means collecting our physical data via devices that can be implanted, swallowed or simply worn, generating huge amounts of health-related information.

Some of these solutions, such as fitness trackers, are an extension of the Internet of Things. But because the Internet of Bodies centres on the human body and health, it also raises its own specific set of opportunities and challenges, from privacy issues to legal and ethical questions.

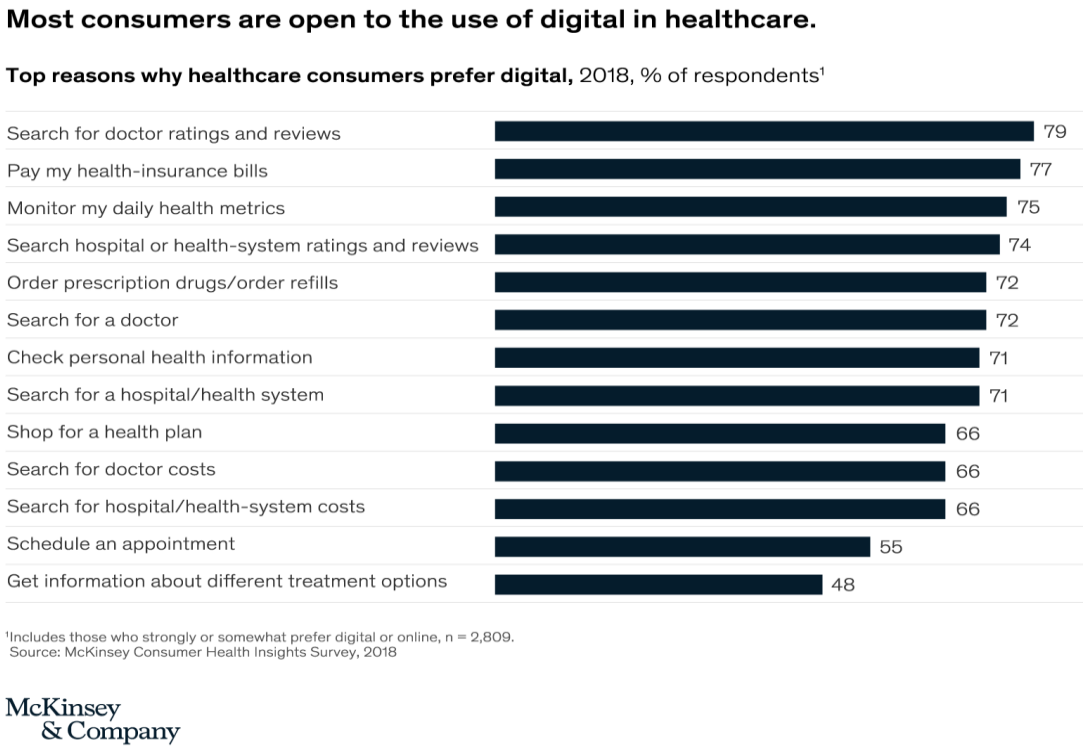


Image: McKinsey & Company

Connecting our bodies

As futuristic as the Internet of Bodies may seem, many people are already connected to it through wearable devices. The smartwatch segment alone has grown into a $13 billion market by 2018, and is projected to increase another 32% to $18 billion by 2021. Smart toothbrushes and even hairbrushes can also let people track patterns in their personal care and behaviour.

For health professionals, the Internet of Bodies opens the gate to a new era of effective monitoring and treatment.

In 2017, the U.S. Federal Drug Administration approved the first use of digital pills in the United States. Digital pills contain tiny, ingestible sensors, as well as medicine. Once swallowed, the sensor is activated in the patient's stomach and transmits data to their smartphone or other devices.

In 2018, Kaiser Permanente, a healthcare provider in California, started a virtual rehab program for patients recovering from heart attacks. The patients shared their data with their care providers through a smartwatch, allowing for better monitoring and a closer, more continuous relationship between patient and doctor. Thanks to this innovation, the completion rate of the rehab program rose from less than 50% to 87%, accompanied by a fall in the readmission rate and programme cost.

The deluge of data collected through such technologies is advancing our understanding of how human behaviour, lifestyle and environmental conditions affect our health. It has also expanded the notion of healthcare beyond the hospital or surgery and into everyday life. This could prove crucial in fighting the coronavirus pandemic. Keeping track of symptoms could help us stop the spread of infection, and quickly detect new cases. Researchers are investigating whether data gathered from smartwatches and similar devices can be used as viral infection alerts by tracking the user's heart rate and breathing.

At the same time, this complex and evolving technology raises new regulatory challenges.

What counts as health information?

In most countries, strict regulations exist around personal health information such as medical records and blood or tissue samples. However, these conventional regulations often fail to cover the new kind of health data generated through the Internet of Bodies, and the entities gathering and processing this data.

In the United States, the 1996 Health Insurance Portability and Accountability Act (HIPPA), which is the major law for health data regulation, applies only to medical providers, health insurers, and their business associations. Its definition of "personal health information" covers only the data held by these entities. This definition is turning out to be inadequate for the era of the Internet of Bodies. Tech companies are now also offering health-related products and services, and gathering data. Margaret Riley, a professor of health law at the University of Virginia, pointed out to me in an interview that HIPPA does not cover the masses of data from consumer wearables, for example.

How is the World Economic Forum addressing challenges raised by the Internet of Bodies?

Another problem is that the current regulations only look at whether the data is sensitive in itself, not whether it can be used to generate sensitive information. For example, the result of a blood test in a hospital will generally be classified as sensitive data, because it reveals private information about your personal health. But today, all sorts of seemingly non-sensitive data can also be used to draw inferences about your health, through data analytics. Glenn Cohen, a professor at Harvard Law school, told me in an interview that even data that is not about health at all, such as grocery shopping lists, can be used for such inferences. As a result, conventional regulations may fail to cover data that is sensitive and private, simply because it did not look sensitive before it was processed.

Data risks

Identifying and protecting sensitive data matters, because it can directly affect how we are treated by institutions and other people. With big data analytics, countless day-to-

day actions and decisions can ultimately feed into our health profile, which may be created and maintained not just by traditional healthcare providers, but also by tech companies or other entities. Without appropriate laws and regulations, it could also be sold. At the same time, data from the Internet of Bodies can be used to make predictions and inferences that could affect a person's or group's access to resources such as healthcare, insurance and employment.

James Dempsey, director of the Berkeley Center for Law and Technology, told me in an interview that this could lead to unfair treatment. He warned of potential discrimination and bias when such data is used for decisions in insurance and employment. The affected people may not even be aware of this.

One solution would be to update the regulations. Sandra Wachter and Brent Mittelstadt, two scholars at the Oxford Internet Institute, suggest that data protection law should focus more on how and why data is processed, and not just on its raw state. They argue for a so-called "right to reasonable inferences", meaning the right to have your data used only for reasonable, socially acceptable inferences. This would involve setting standards on whether and when inferring certain information from a person's data, including the state of their present or future health, is socially acceptable or overly invasive.

Practical problems

Apart from the concerns over privacy and sensitivity, there are also a number of practical problems in dealing with the sheer volume of data generated by the Internet of Bodies. The lack of standards around security and data processing makes it difficult to combine data from diverse sources, and use it to advance research. Different countries and institutions are trying to jointly overcome this problem. The Institute of Electrical and Electronics Engineers (IEEE) and its Standards Association have been working with the US Food & Drug Administration (FDA), National Institutes of Health, as well as universities and businesses among other stakeholders since 2016, to address the security and interoperability issue of connected health.

As the Internet of Bodies spreads into every aspect of our existence, we are facing a range of new challenges. But we also have an unprecedented chance to improve our health and well-being, and save countless lives. During the COVID-19 crisis, using this opportunity and finding solutions to the challenges is a more urgent task than ever. This relies on government agencies and legislative bodies working with the private sector and civil society to create a robust governance framework, and to include inferences in the realm of data protection. Devising technological and regulatory standards for interoperability and security would also be crucial to unleashing the power of the newly available data. The key is to collaborate across borders and sectors to fully realize the enormous benefits of this rapidly advancing technology.

What is the Internet of Bodies (IoB), and why should you care?

The Internet of Bodies (IoB) term was coined in 2016. It describes connected devices that monitor the human body, collect physiological, biometric, or behavioral data, and exchange information over a wireless or hybrid network. Standalone mobile apps that analyze physical activity and health-related data, such as heartbeat, blood pressure, and sleep cycles, can also be considered part of the IoB cohort. However, we've deliberately excluded them from our classification to avoid confusion with mHealth.

The Internet of Bodies falls under the broader IoT solutions umbrella. But as the name implies, IoB devices ensure an even closer synergy between humans and gadgets than connected thermostats, refrigerators, and curtains.

IoB products come in various forms, ranging in complexity from smartwatches and fitness trackers, which are used by approximately 21% of Americans, to implantable insulin delivery systems, ingestible sensors, and brain stimulation gadgets.

The benefits of implementing IoB solutions at scale include better diagnosis and treatment of health conditions, personalized insurance plans, increased productivity, and improved public safety, to name a few.

But the growing Internet of Bodies adoption could also result in unauthorized access to sensitive information by third parties, income-based health disparities, and the installment of a global surveillance state.

This article will take a closer look at IoB benefits and applications in the healthcare and wellness domains and identify privacy and security concerns surrounding the Internet of Bodies and medical IoT solutions. So let's dive right in!

What is the Internet of Bodies exactly?

Just like other members of the Internet of Things family, IoB devices operate on four levels:

- **Hardware** with limited or advanced computing capabilities. IoB devices are enhanced with embedded software and an array of sensors measuring human-generated data (step count, pulse, oxygen levels, hematological parameters, facial features, or daily routines.) Depending on a gadget's processing power, sensor data can be stored and analyzed either on the device or in the cloud. It is possible to combine invasive and wearable IoB devices into a wireless body area network (WBAN).
- **Networks**, which can be wireless or hybrid. Connectivity technologies allow IoB systems to securely exchange data with each other and a central hub at preset intervals or in real time.
- **Back-end infrastructure**, which encompasses data storage, analytics, and visualization solutions. When it comes to IoB, the "infrastructure" team can also refer to a support system ensuring a gadget's uninterrupted operation, such as a team of healthcare specialists ready to intervene should a personal help button be pressed.
- **End-user applications** that allow individuals to configure IoB devices, connect them to other hardware and apps, and view sensor data over a given period. These apps often run on mobile devices, although voice interfaces are also getting traction in the Internet of Things domain.

To classify as the Internet of Bodies product, connected devices must perform one or both of these functions:

- Gather health, behavioral, or biometric data
- Alter the human body's functions

Most IoB products come in direct contact with the human body, are physically attached to it, or, as in the case of ingestible and implantable devices, are swallowed or surgically inserted into a patient's system.

Subsequently, the U.S. Food and Drug Administration (FDA) heavily regulates the development, manufacturing, and use of the Internet of Bodies solutions. Even consumer wearables, which previously were not considered medical devices unless manufacturers labeled them so, now often require FDA clearance. While this might slow down the launch of certain IoB products and features, such as the oximeter functionality introduced in Apple Watch when the pandemic struck, the decision also prevents flawed devices from entering the market and causing damage to people's health.

Examples of IoB products

For your convenience, we've divided the Internet of Bodies solutions into two categories — i.e., consumer-grade and medical devices.

Consumer IoB device

Connected home solutions

- Security cameras and door locks with face recognition capabilities

- Voice-controlled smart home devices
- Automatic pill dispensers
- Hearing aids
- Indoor navigation systems for the visually impaired
- In-home remote monitoring systems for the elderly and patients with chronic conditions

Fitness devices

- Wearable physical activity trackers, including innovative accessories
- Fitness mirrors with computer vision functionality
- Connected fabrics and apparel
- Training and weight measuring equipment enhanced with sensors

Wellness technology

- Baby tech solutions: camera and sensor-based monitors, smart cribs, intelligent baby formula makers, and connected body temperature thermometers and nebulizers
- Femtech products: smart pads, tampons, and menstruation cups; connected bras and breast cups, hardware-based fertility trackers, pelvic floor training tools
- Vitals monitoring devices: wearables for heart rate, blood pressure, and oxygen monitoring
- Diabetes management systems: smart glucose meters, wearable insulin pumps, and sensor-infused medication storage devices

Medical IoB devices

Smart hospital solutions

- Biometric-based identification systems for patients and hospital staff
- Connected hospital beds with vitals monitoring functionality
- Point-of-care testing equipment
- Stationary medication dispensers
- Integrated IoT systems for inpatient, outpatient, and remote patient care

Implantable and ingestible devices

- Organ systems: heart implants, artificial pancreas systems, smart stents, cochlear implants for individuals with hearing loss, artificial retina implants
- IoT-based prosthetic limb systems
- Neurological IoB solutions: brain-computer interfaces (BCI) with implantable sensors, deep brain stimulation solutions, seizure monitors
- Digital pills for non-invasive diagnostic procedures and medication intake monitoring

How the Internet of Bodies revolutionizes healthcare

Although the Internet of Bodies can transform nearly every industry, healthcare professionals are the immediate beneficiaries of the IoB revolution.

The advantages of adopting IoB products in medical care span:

- **24/7 patient monitoring**. Sensor and camera-based IoT devices allow caregivers to spot the slightest changes in patients' physiological data, anticipating their decline and taking immediate action in emergency cases. Additionally, IoB technologies help reduce physical interactions between patients and medical personnel, thus preventing contagious diseases from spreading.
- **Non-invasive diagnosis**. While sensor data collected by a smartwatch can itself provide valuable insights into a patient's past, current, and future health conditions, IoB also offers a variety of tools for non-invasive and highly efficient medical diagnosis. Camera-based ingestible pills, for example, serve as a viable alternative to gastroscopy and colonoscopy. A sleek wearable gadget worn at the lower part of the ribcage can monitor lung function and flag abnormalities early on. And by analyzing data collected through wearable sweat sensors, physicians can diagnose genetic disorders and better treat diabetes.
- **Improved quality of life for patients with chronic conditions**. Unlike wearables, which merely collect data, implantable and embedded IoB products can change and restore the body's functions that have been affected by physical trauma or disease. Some examples of such devices include connected pacemakers that transmit data to a dedicated mobile app, microelectronic retina prostheses returning partial vision to people with retinal diseases, and automated insulin delivery systems monitoring blood sugar levels in real time.
- **Precision medicine**. IoB devices could help healthcare professionals identify recurring patterns in health data and devise personalized medicine and treatment plans tailored to the needs of a particular patient or patient group. For this purpose, electronic health records (EHRs) could be augmented with sensor data and analyzed using artificial intelligence algorithms.

- **Personalized health insurance plans**. The data obtained from the Internet of Bodies products allows health insurance companies to adopt a more granular approach to risk profiling and optimize insurance plans based on an individual's medical history, occupation, and lifestyle. Besides driving patient engagement and encouraging users to pursue a healthy lifestyle, the growing adoption of IoB solutions in medical insurance could reduce hospitalization rates and cut claims processing and administrative costs by up to 40%.

A rundown of IoB challenges and risks — and ways to address them

Privacy

In addition to users' whereabouts, IoB devices can track various body parameters, such as cardiac rhythms, sleep patterns, and menstrual cycles. And it's not completely clear who can access and use this information.

The biometric data captured by an implantable cardiac device, for example, could serve as evidence in disputable criminal cases, like the infamous Ross Compton lawsuit. In 2016, the police obtained information from Mr. Compton's cardiac pacing devices when suspicions around whether a critically ill man could escape a fire while neatly packing his belongings into a suitcase had arisen.

Another example comes from Amazon. The company's questionable treatment of employees during the pandemic hardly comes as a surprise following the introduction of arm motion trackers for warehouse workers. The intrusive

technology would potentially allow Amazon to detect idling employees and collect personal information, such as the frequency of their bathroom breaks.

A comprehensive legal framework is necessary to establish crystal-clear guidelines for collecting, analyzing, and using physiological, behavioral, and biometric data produced by IoB devices. Until then, the Internet of Bodies vendors are expected to comply with HIPAA, FTC, FIPPs, FCRA, and GLBA regulations.

Security

Being part of the larger Internet of Things family, IoB devices may contain the very same security vulnerabilities as compromised baby monitors talking in weird voices and hacked CCTV cameras that fall victim to malware attacks and attempt to bring the whole Internet down. These vulnerabilities may spana cumbersome software updates installation process, hard-coded and easy-to-guess passwords, the use of insecure or outdated software and hardware components, and a failure to encrypt data traversing the network, among others. And while it literally won't kill you if your fitness tracker joins a newly formed botnet, a hacked cardiac implant or insulin pump is a totally different story.

To prevent businesses, cybercriminals, and foreign governments from accessing sensitive data and launching high-profile cyberattacks on the US IT infrastructure, the FDA must devise a comprehensive IoB cybersecurity framework, which could be based on the corresponding framework developed by the National Institute of Standards and Technology. Additionally, the FDA could impose stricter security requirements on IoT companies from the fitness and wellness segments.

Ethics

Without proper regulations, individuals who use IoB devices may not fully own biometric data. In addition, when implemented in public settings like schools and hospitals, the Internet of Bodies solutions might inadvertently monitor other people surrounding the user, which violates their privacy. And as more healthcare providers and insurance companies incorporate wearable data into treatment plans and health coverage, individuals with lower incomes and limited access to technology may end up missing out on IoB benefits.

One way to tackle these problems could be to conduct extensive research on IoB risks and benefits and make the information publicly available, thus filtering out the marketing hype. Closer collaboration between policymakers and device manufacturers could also help address data privacy concerns and make IoB products more affordable.

What's in store for the Internet of Bodies solutions?

The pandemic sparked the general public's interest in digital healthcare solutions, and healthcare providers have followed suit. Driven by telehealth, remote patient monitoring, and healthcare analytics solutions, the digital health market is on track to top $220 billion by 2026.

And it's only a matter of time before the Internet of Bodies goes mainstream too.

On the one hand, we're witnessing the emergence and at-scale implementation of innovative networking technologies, including satellite Internet, Wi-Fi 6, and 5G. The latter, for instance, could potentially support up to one million devices per square kilometer (up from 4,000 devices per square kilometer for 4G networks.)

On the other hand, we could soon expect greater interoperability between IoT and IoB devices, which will exchange data in a unified format and at a faster speed. Several critical steps, such as the establishment of the global one M2M initiative, have already been made in this direction.

All of this would create next-gen cyber-physical systems where connected thermostats feed off data collected through sensors embedded into smart apparel, automatically adjust their temperature settings, and notify an endocrinologist if glucose concentration in your sweat goes up.

ARTIFICIAL INTELLIGENCE CYBERSECURITY HEALTH TECHNOLOGY

What is the Internet of Bodies?

Beyond Smartwatches and Pacemakers, New Devices Collect Biometric Data with Patchy Regulation

Wearable, ingestible and implantable devices might know if you drank too much last night, didn't take your meds or aren't paying attention. Who's regulating them?

Journalists should distinguish between “Internet of Bodies” medical devices that are regulated by the Food and Drug Administration, and consumer devices that are mostly unregulated – and may pose privacy, cybersecurity and equity risks, Mary Lee of the RAND Corporation told NPF data privacy fellows.

4 TAKEAWAYS:

① **Connected devices that collect data on the human body are evolving into an ecosystem.** The “Internet of Bodies” is a subset of the Internet of Things that collects a person’s health or biometric data (like an Apple Watch or Fitbit) or alters the human body’s function (like a smart insulin pump, explained Mary Lee, a mathematician at the RAND Corporation. They include watches, rings and smartphone apps that track steps, heart rate and maybe how much alcohol you drank last night. There are also attention monitors – glasses that use brain activity and eye movements that might vibrate if they think you’ve spaced out. I’ve heard of them being used in schools in China to make sure that students are paying attention,” Lee said.

② **Implantable and ingestible devices are (usually) regulated by the FDA but consumer devices are not.** These include pacemakers that upload data to a cardiologist and pills that contain sensors that record

whether medication was taken. So far, pills that transmit to a mobile app for patient compliance have been approved for schizophrenia and chemotherapy. These medical devices are regulated by the FDA and must adhere to guidelines that cover privacy and cybersecurity.

Lee is concerned that they may improve health outcomes but widen inequality in healthcare treatment. Moreover, she noted the recent spate of ransomware attacks on hospitals that have exposed patient data. Finally, the FDA has begun to regulate some software.

"There's FDA-approved apps on your watch, which is the consumer device but has some medical angles to it. To me, the landscape is a little bit murky and confusing right now," Lee said.

③ **There are plenty of fascinating angles for journalists to explore.** Lee flagged a number of unanswered questions, including: Can we be free from the Internet of Bodies, as devices can be used to track people without their consent? What are the rules governing employer use of devices to track their employees, or authorities using ankle monitors to track incarcerated people or immigrants awaiting a hearing under the ICE "alternative to detention" program?

“Then there’s the question of body autonomy and integrity,” Lee said. “Once a device is implanted inside of you, for example, are you free to modify it as you like once it’s inside your body? What does that mean in terms of software end-user license agreements?… Will the device still be under warranty, for example, if you mess with it but it’s a part of you?”

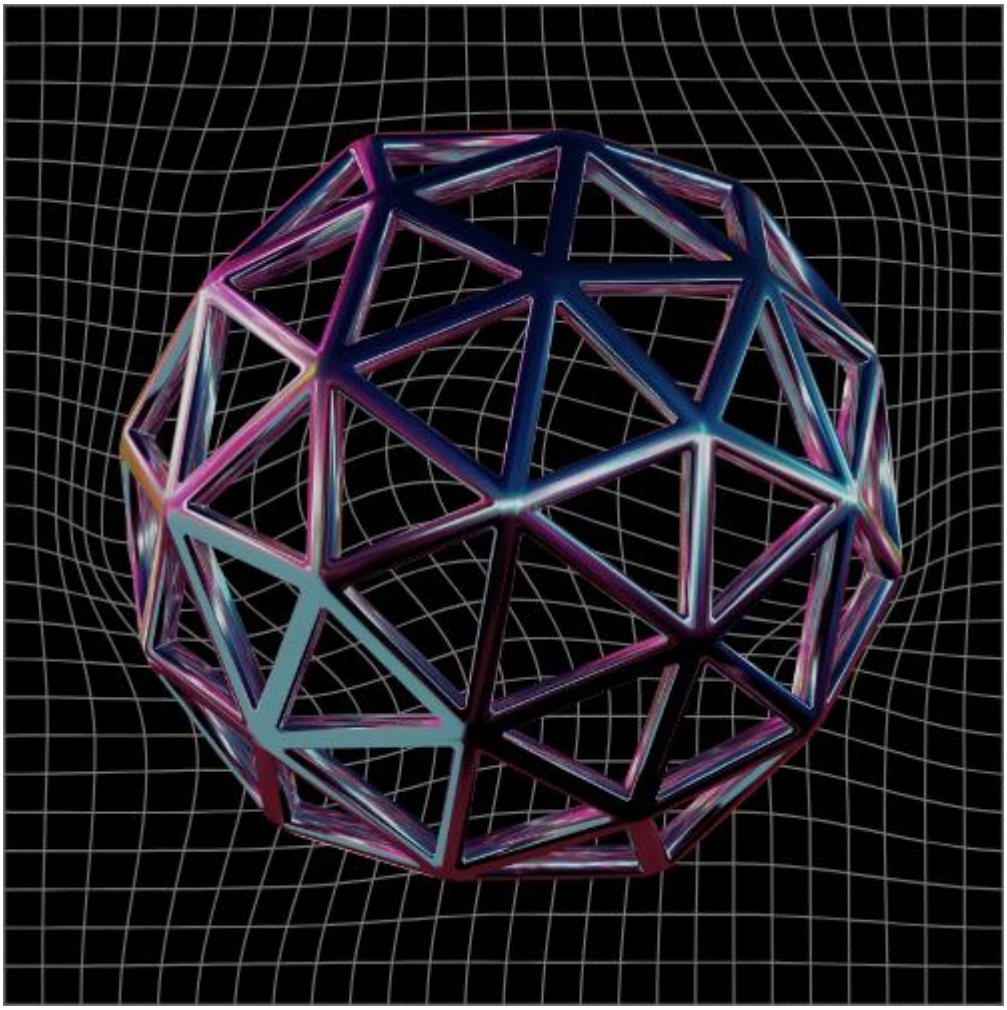
The courts have yet to weigh in, Lee noted. In Ohio, police issued a warrant for the pacemaker records of a man named Ross Compton, who was charged with arson when his alibi did not match his heart data. Compton’s lawyers objected, but a judge ruled the pacemaker data was admissible at trial. Compton died before the appeals court could rule on the matter, so there is no legal precedent now, Lee said.

④ **Are we ready for this?** There is a patchwork of regulations and state laws, including efforts to regulate data brokers, and some voluntary security standards, but Internet of Bodies technology is moving faster than the policy can keep up. “In my mind, the question is, the Internet of Bodies is already here, but are we ready for its implications? Lee said.

An Introduction

What is Internet of Bodies (IoB) used for?

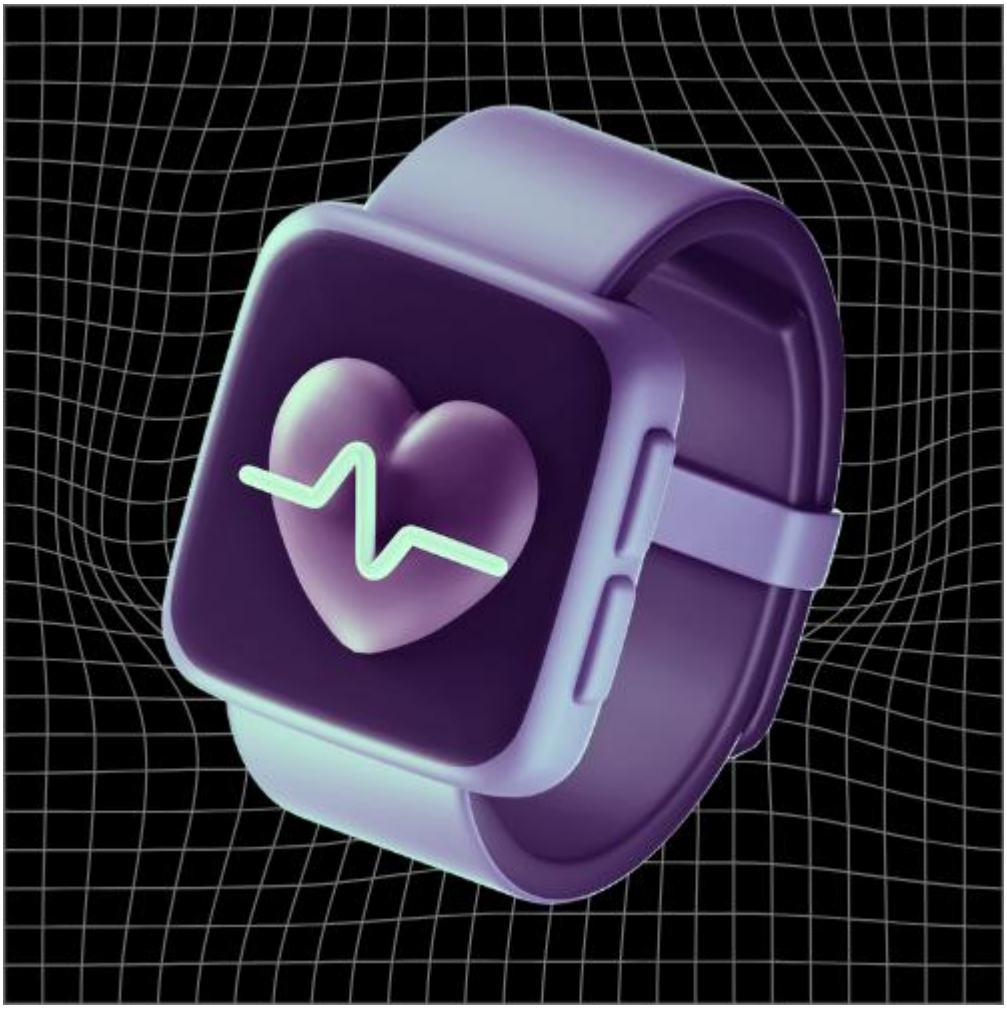
CONNECTIVITY



Human body communication (HBC) can provide highly secure and power-efficient data transmission among wearable, implanted, and ingested medical devices, KAUST researchers have shown.

"The IoB is a network of wearable, implantable, ingestible and injectable smart objects that allows for in-, on- and off-body communications," says Ahmed Eltawil from IEEE (Institute of Electrical and Electronics Engineers).

HEALTH MONITORING



IoB can collect physiological or behavioral data on the human body and share it with healthcare providers.

These data include **vital signs, movements, sleep patterns, brain activity,** and more.

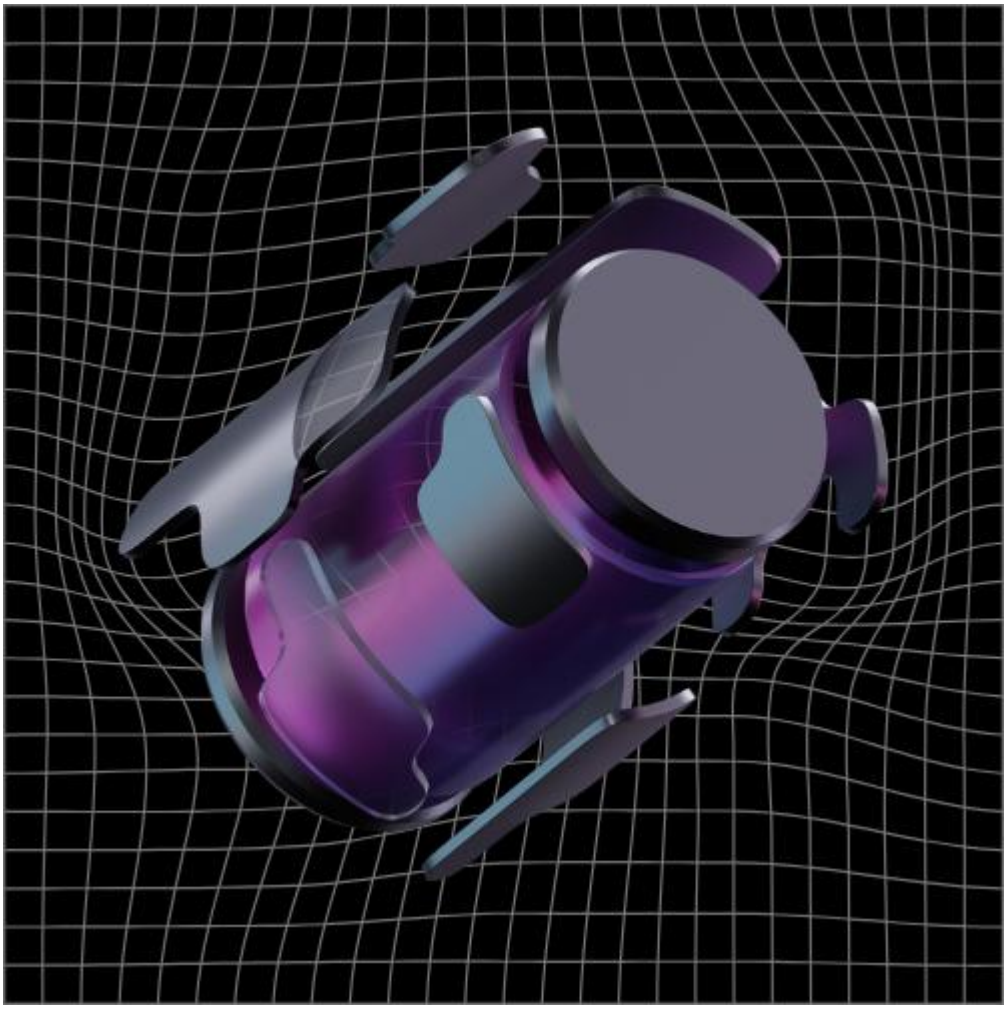
By collecting real-time data on a person's health and behaviors, IoB can detect anomalies at their very earliest stages. It also helps in compliance and prognosis as it empowers patients to track their own health and wellness, optimize their performance, and enhance their quality of life.

DATA COLLECTION & ANALYTICS

Machine learning, AI, and other data science techniques are used in addition to traditional statistics to recognize patterns and make predictions based on— large, empirical data sets.

(Person-generated health data) PGHD collected by IoB devices allow for continuous monitoring of health status in real time, as well as collection of longitudinal data outside of—or in addition to—the intermittent monitoring that takes place in clinical settings.

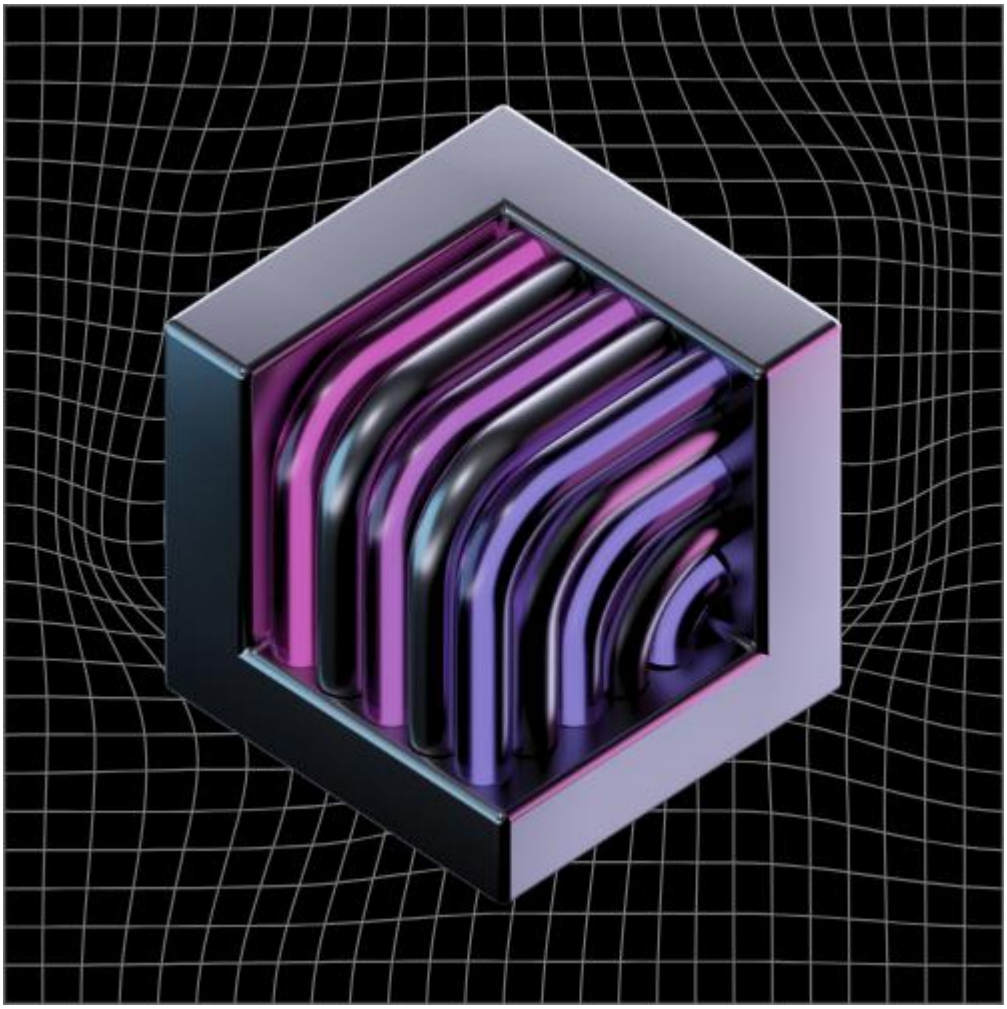
PERSONALIZED MEDICINE & THERAPY



Interconnecting the architecture of people, sensors, apps, and devices creates heterogeneous data and projects a "Precision Medicine" approach.

Precision Medicine improves the quality of treatment via cutting an extra cost associated with inaccurate/unnecessary diagnoses, medications, and care plans. Moreover, reduces medical errors and designs preventive care for patients with similarities in medications, conditions disease presentations.

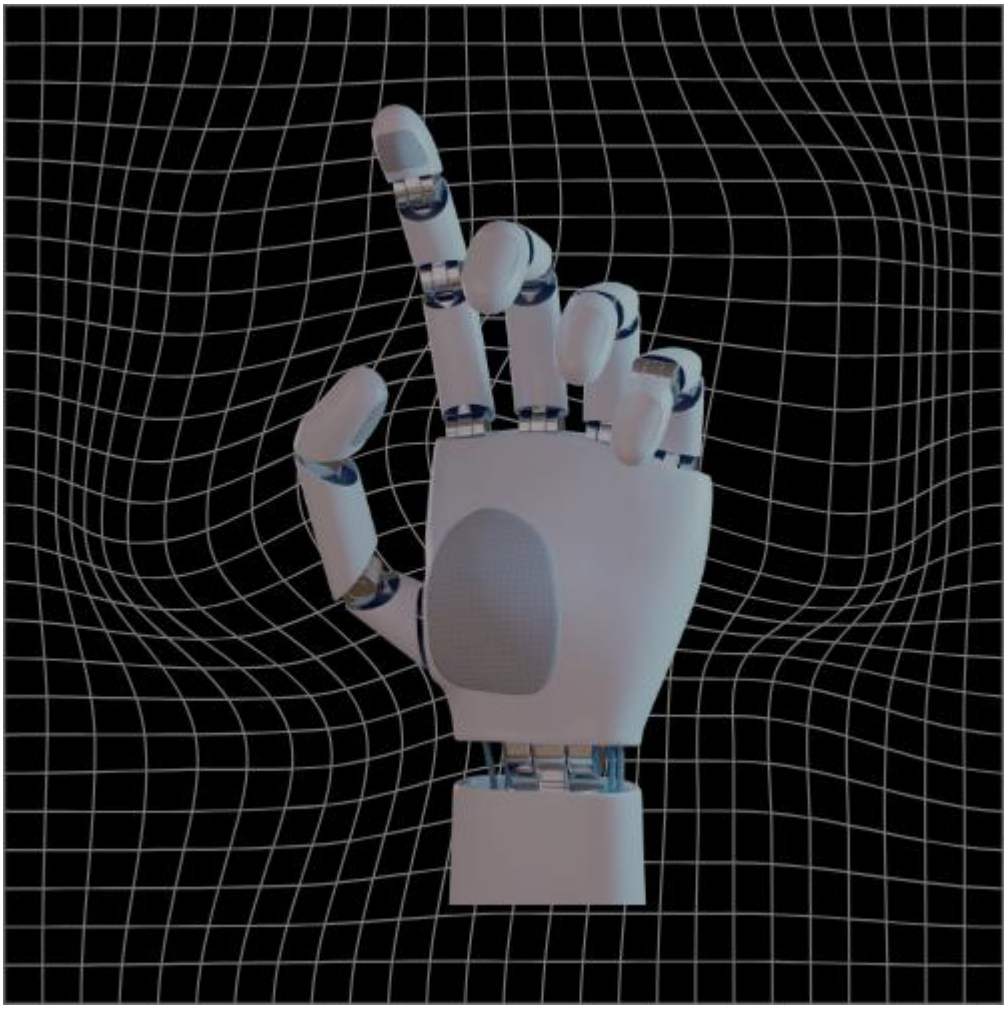
SECURITY AND DATA



Embedded technologies will allow us to hold our own data within our own bodies—not on a server or a metaverse owned by profiteers, not taken from a wearable that sells our body data with no return to us.

Implants can attach our data to us, ensuring it is part of us. The Internet of Bodies visions an interconnectivity led by our bodies and our identities, where our transmission and reception of data exist within co-created virtual physical space, where our physical selves are 'tethered' to our data selves.

BIO-ENHANCEMENT & AUGMENTATION



The Internet of Bodies opens up the possibility of augmenting human capabilities through direct integration with technology.

Brain-computer interfaces (BCIs) could potentially enable individuals to control external devices or even robotic limbs using their thoughts alone.

Advancements of biomedical engineering in neuroscience resulted in the development of neuroprosthetics that has been used as assistive and restorative apparatuses in disabilities.

Wireless Body Area Network (WBAN)

WBAN technology is a cornerstone of the Internet of Bodies (IoB), a concept that connects human bodies to the digital ecosystem.

It consists of sensors that are placed in different parts of the body and can be wearable or implanted under the users' skin. These communicate with a special coordinator node and are responsible for sending biological signals of the patient to the medical doctor in order to provide real time medical diagnostics and allow them to take the right decisions.

WBAN Applications

Telemedicine and remote patient monitoring

Rehabilitation and therapy

Biofeedback

Ambiant Assisted Living

HIERARCHY OF DEVICES IN IoB ECOSYSTEMS

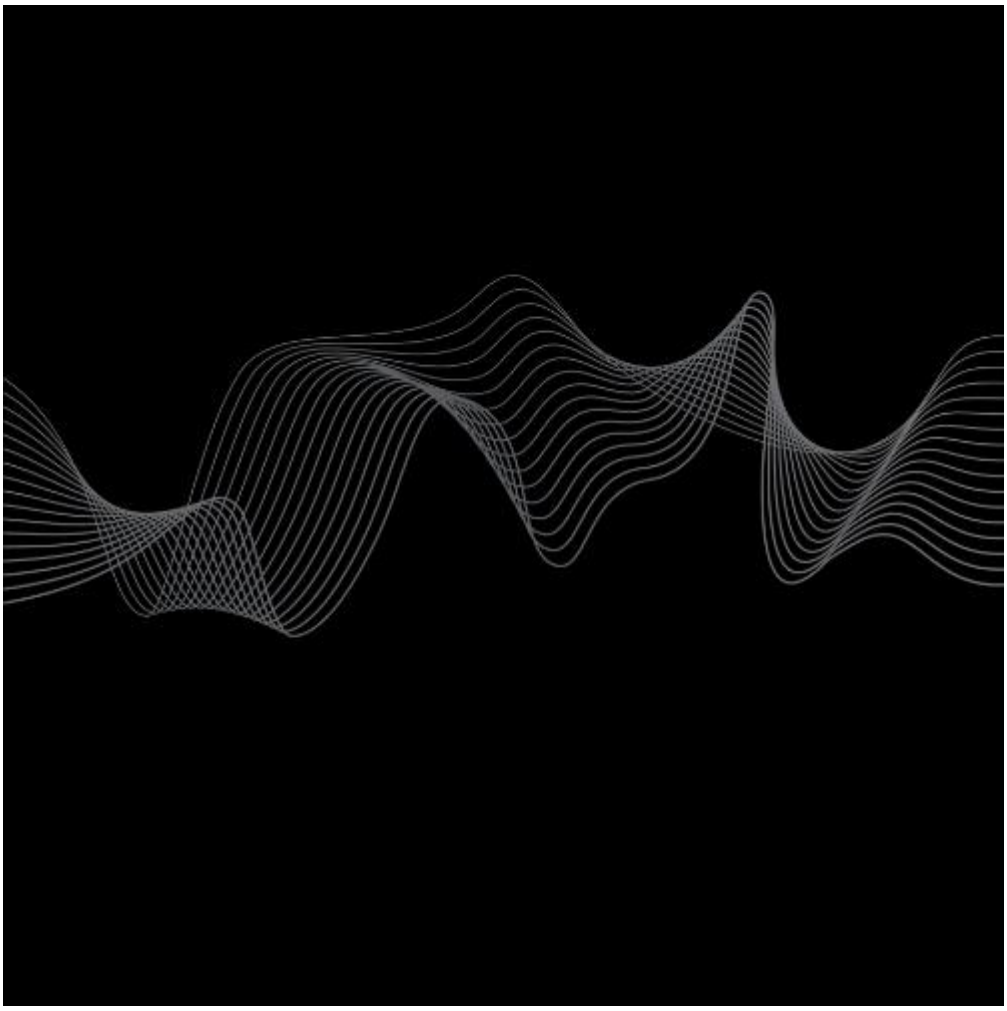
- **First Generation/ Body External:**

  Worn or physically connected to a human body.
- **Second Generation/ Body Internal:**

  Placed internally in a human body. They may be ingested or surgically implanted.
- **Third Generation/ Body Embedded:**

  Electronic devices may be completely merged with the human body.

As of now, the first generation of external devices is widely in practice and internal devices in their various forms are slowly gaining traction.



THE BODY AS A SOURCE OF DATA

IoB gadgets operate on different levels:

Hardware: Implies computing capabilities that are required to operate data and internal gadget's memory/cloud used for data storage.

Networks: Connection between IoB gadgets is required for the secure data exchange.

Back-end: Unifies storage, analytical, and rendering solutions; may even include a support team that controls the smooth functioning of the gadget.

End-user apps: Serves the configuring for IoB devices; Allows users to view information for a certain period, and may be connected with hardware or other applications.

We've refreshed our look and upgraded your experience, but as we settle in, you might notice a few hiccups. Thank you for your patience as we fine-tune things—there's much more to come.

Meeting the Future: Internet of Bodies

- Last Updated: December 2, 2024

The global internet of things (IoT) in healthcare market is projected to grow to $446.52 billion by 2028, according to Fortune Business Insights. Integration of IoT technologies and medical care drive exciting innovations, resulting in more effective healthcare solutions. One of these new innovations is the *Internet of Bodies*. Let's find out exactly what it is and the ways in which it can revolutionize our lives.

'From providing automated, remote patient care, to increasing community engagement in self-health management, the Internet of Bodies brings technology innovations to improve living standards.' - MobiDev

What is the Internet of Bodies?

In recent years, the healthcare industry has been undergoing significant technology-related changes. Several of these changes include the use of augmented reality applications to assist doctors during surgery, the introduction of AI to improve the efficiency of diagnostic processes and, of course, the surge of IoT devices that are becoming more widespread. This list would be incomplete without the Internet of Bodies.

IoB gadgets are wearable, ingestible, or implantable. We can consider IoB as an ecosystem of devices that are connected to the Internet. Following the Web of Things concept, IoB enhances the interoperability and connectivity of smart devices by standardizing communication protocols between different IoT smart devices. In healthcare, they gather crucial data at the core of precision medicine. This enables accurate treatment for the needs of the particular person.

Having first appeared in 2016, the term the Internet of Bodies (IoB) came into general use, bringing together all devices that monitor the human body. Some devices include the following:

- Hearing aids
- Ingestible sensors
- Wearables for heart rate

Outside of healthcare, IoB products are also used as commercial devices. This can include any of the following:

- Surveillance cameras
- Locks actuated via face recognition
- Voice-controlled devices for home
- Navigation/wellness gadgets

The Body as a Source of Data

The possibility to perceive the body as the source of data lies in the core of IoB. The concept isn't fully clear, though it appears to be a promising perspective.

The Internet of Bodies is classified as a variety of IoT that enhances engagement between devices and our bodies. Its widespread implementation improves the accuracy of treatment as well as human well-being. For example, the device has the capability to automate insulin dosing for diabetics. Other advantages of IoB implementation include possibilities to personalize insurance plans, improve performance, and develop preventative healthcare.

However, the type and amount of received data depends on the IoB gadget and its operation on different levels:

- **Hardware**: Implies computing capabilities that are required to operate data, from step count to medical indicators; Internal gadget's memory, or the cloud, is used for data storage
- **Networks**: Connection between IoB gadgets is required for the secure data exchange
- **Back-end**: Unifies storage, analytical, and rendering solutions; Represents an infrastructure that may even include a support team that controls the smooth functioning of the gadget
- **End-user apps**: Serves the configuring for IoB devices; Allows users to view information for a certain period, and may be connected with hardware or other applications

Types of IoB Solutions

In regards to the classification of IoB gadgets, there are three generations:

1. **External** (outside of body): Work to monitor daily activity and vary from wristbands to smartwatches.

2. **Internal** (inside of body): Includes implanted devices like a pacemaker, cochlear, or an organ developed with the help of a 3D printer.
3. **Body-fused**: May be equipped with communication modules to interpret biological parameters and be connected to remote machines in a real time. The typical example is a "smart" pill. After swallowing, embedded chips inside the pill measure and transmit parameters to the head device. The first smart pill was approved by the Food and Drug Administration in 2017. It is currently being used for patients who have psychiatric and other illnesses.

Application of IoB can become one of the main trends in healthcare, enabling 24/7 monitoring of health and obtaining full statistics related to any deviation from standard criteria.

Internet of Bodies Use Cases

Wristband

The IoB wristband works to send ultrasonic pulses to check hand movements and the location of an employee. The device vibrates if lack or total absence of activity is recorded. Implementation of such a device in the workplace improves productivity. Also, it helps help companies care more about the health of their employees, which is the number one priority for everyone in the post-COVID-19 world.

Implantable Cardiac Device

These IoB devices are implanted in the chest and connected with the heart. The transmitter located in the user's house receives data regarding the heart's functioning and transfers information to the doctor. Moreover, the device normalizes heartbeat and treats health problems.

COVID-19 Patients

Internet of Bodies helps to monitor patients in terms of COVID-19. For example, doctors in China have been using digital thermometers to monitor the patient's temperature without contacting them. Digital thermometers prevent the spread of COVID-19 and are combined with other IoB devices for real-time monitoring to provide remote control and diagnostics.

BCIs

An embedded device, the Brain-computer Interfaces (BCIs), may be considered as a breakthrough since it allows users to control devices via brain signals and significantly improves lives of people with disabilities.

Monitoring of Athletes/Soldiers

In healthcare, IoB use cases are still the most common. But we continue to see IoB gadgets being used in other areas, such as sports and even the military. There are now wearables that monitor the performance of athletes can take other forms. Military IoB use cases include the monitoring of soldiers by tracking their emotional and physical state, location, and current condition. Simulation of combat situations serves as a source of data that describes the reaction of the body in critical conditions.

Challenges and Risks of IoB Adoption

IoB adoption is closely associated with the potential risks of stolen information. This can be collected and misused, leading to the disruption in the normal functioning of a device. The potential threats are similar to those of other IoT devices, but risks are higher since IoB devices are connected to the body and its functioning. The number of risks is increased if IoB cybersecurity modules aren't effective, or if data encryption approaches are outdated.

Proper regulations must also be ensured, and the people who apply IoB devices must fully own biometric data, so the devices are not adopted in public settings. If they are, they may begin to monitor people around the user, violating the privacy regulations. A prominent example of a privacy violation is Amazon's solution. The company introduced arm motion trackers for employees in warehouses. But this is a violation of privacy, as they were collecting personal information about the workers.

Overall, the future of IoB is blurred, but the number of IoB use cases continues to grow. From providing automated, remote patient care, to increasing community engagement in self-health management, the Internet of Bodies brings technology innovations to improve living standards. If risks and rewards are balanced, IoB devices will become an integral part of our lives.

What Is The Internet Of Bodies? And How Is It Changing Our World?

Have you heard the term the Internet of Bodies (IoB)? That may conjure up a few thoughts that have nothing to do with the true nature of the term, but it's about using the human body as the latest data platform. At first, this concept seems quite creepy, but then when you realise the possibilities it creates, it becomes quite exciting. Here we explore what the Internet of Bodies is, some examples in use today, and a few of the challenges it presents.

What is the Internet of Bodies (IoB)?

When the Internet of Things (IoT) connects with your body, the result is the Internet of Bodies (IoB). The Internet of Bodies (IoB) is an extension of the IoT and basically connects the human body to a network through devices that are ingested, implanted, or connected to the body in some way. Once connected, data can be exchanged, and the body and device can be remotely monitored and controlled.

There are three generations of Internet of Bodies that include:

- Body external: These are wearable devices such as Apple Watches or Fitbits that can monitor our health.
- Body internal: These include pacemakers, cochlear implants, and digital pills that go inside our bodies to monitor or control various aspects of our health.
- Body embedded: The third generation of the Internet of Bodies is embedded technology where technology and the human body are melded together and have a real-time connection to a remote machine.

Progress in wireless connectivity, materials, and tech innovation is allowing implantable medical devices (IMD) to scale and be viable in many applications.

Examples of Internet of Bodies Devices in Use or Development

The most recognised example of Internet of Bodies is a defibrillator or pacemaker, a small device placed in the abdomen or chest to help patients with heart conditions control abnormal heart rhythms with

electrical impulses. In 2013, former United States Vice President Dick Cheney got his WiFi-connected defibrillator replaced with one without WiFi capacity. It was feared that he could be assassinated by electric shock if a rogue agent hacked the device.

A “smart pill” is another IoB device. These pills have edible electronic sensors and computer chips in them. Once swallowed, these digital pills can collect data from our organs and then send it to a remote device connected to the internet. The first digital chemotherapy pill is now in use that combines chemotherapy drugs with a sensor that captures, records, and shares information with healthcare providers (with the patient’s consent) regarding the drug dosage and time, plus other data on rest and activity, heart rate and more.

“Smart contact lenses” are being developed that integrate sensors and chips that can monitor health diagnostics based on information from the eye and eye fluid. One smart contact lens in development aims to monitor glucose levels that will hopefully allow diabetics to monitor their glucose levels without repeated pinpricks throughout the day.

Taking it up a notch is the Brain-Computer Interface (BCI), where a person’s brain is actually merged with an external device for monitoring and controlling in real-time. The ultimate goal is to help restore function to individuals with disabilities by using brain signals rather than conventional neuromuscular pathways.

But not all Internet of Bodies use cases are for healthcare reasons. Bioengineering company, Biohax has embedded chips in more than 4,000 people primarily for convenience. In one widely reported example, 50 employees of Three Square Market agreed to have an RFID microchip the size of a large grain of rice (similar to what’s embedded in pets to be able to identify and locate them when they are lost) implanted. This chip allows these employees to gain access to the building without a key, pay for items with a wave of their hand at the vending machine by deducting the amount immediately from their account rather than use money and log onto their computers.

Challenges Faced by Internet of Bodies Technology

The situation of U.S. Vice President Cheney getting a defibrillator not connected to WiFi for security reasons illustrates one of the biggest challenges faced by Internet of Bodies technology—how to secure the devices and information they collect and transmit. Nearly half a million pacemakers were recalled in 2017 by the U.S. Food and Drug Administration over security issues requiring a firmware update. The security challenges faced by Internet of Bodies tech are similar to what plagues Internet of Things generally, but there can be life and death consequences when IoB devices are involved. Additionally, IoB devices create another cyber security challenge that will need to be safeguarded from hackers.

Privacy is also of paramount concern. Questions about who can access the data and for what purpose need answers. for example, a device that monitors health diagnostics could also track unhealthy behaviours. Will health insurance companies be able to deny coverage when a customer’s IoB device reports their behaviour? A cochlear implant could restore hearing, but it might also record all audio in a person’s environment. Will that data remain private?

As Internet of Bodies tech continues to grow, regulatory and legal issues will have to be resolved and policies built around the proper use of the technology.

30 January 2023

How human are you? The Internet of Bodies is here, but are we ready?

Miles Harmsworth considers the next generation of IoB devices and the approach to regulating them.

by **Dr. Paul Voigt, Lic. en Derecho, CIPP/E**

Recent leaps in neurotechnology signal a distinct shift from a world in which we 'use' technology, to one where we 'become' the technology. The third generation of the Internet of Bodies is approaching, so what exactly is it, what are the legal issues, what are countries doing (or not doing) to get ahead of the game and why is the UK taking a different approach to some of its global counterparts?

What is the Internet of Bodies?

Internet-connected devices like smart fridges, video doorbells and voice assistants are all examples of the Internet of Things (IoTs) – smart devices that connect and communicate through a network.

The Internet of Bodies (IoB) describes a sub-set of IoT devices that interact far more intimately with the human body. They connect the body to an online network through technology that you can wear, ingest, implant or otherwise link to a human body. IoB devices fall into three categories:

- **External devices / 1st gen** – these are devices that you can wear and that collect and transmit data using external sensors, such as smart watches.

- **Internal devices / 2nd gen** – these are devices that you can ingest or have implanted to control and monitor various aspects of your health, such as digital pills and smart pacemakers.
- **Embedded devices / 3rd gen** – these are devices that completely merge with your body while maintaining a real-time connection to a remote machine, such as a brain computer interface (BCI).

External and internal devices are already commonplace but embedded devices are the next frontier. With Elon Musk proclaiming at the latest Neuralink 'Show and Tell' event that the first chip will be installed in a human by June 2023, now is a prime time to consider the impact of such devices.

What are BCIs?

BCIs are the most talked embedded device to date – these are devices that merge with the human brain, allowing for a real-time connection with remote computers that receive live data updates for the purposes of controlling and monitoring aspects of human health.

BCIs offer the first real step towards uniting humans and artificial intelligence. Their functionality extends far beyond the health stats you'll be familiar with on your smartwatch. They have the potential not only to track our data and provide assistive support, but also to enhance our body's functions – the Milken Institute predicts that AI BCIs could unlock cures to health conditions that have phased scientists for decades, including Alzheimer's and Parkinson's disease, and we are quickly seeing companies line up to deliver:

- **Synchron**, is an Australian-based neurotechnology company that was first to gain FDA approval to conduct human trials for BCIs, and has already successfully enabled paralysed patients to send emails and text messages.
- **Neuralink** is a Californian-based neurotechnology company that is designing devices that will restore sight in blind people and the ability of those with severed spinal cords to walk. As at the date of this article, Neuralink is awaiting FDA approval to start human trials.

For those currently suffering from severe health conditions, BCIs can't come soon enough, but such technological leaps are not generally characterised by sunshine and rainbows, and if the Borg in Star Trek are anything to go by, it's worth considering the potential downsides and how we can mitigate them.

The price of progress?

In August 2022, the UK Law Society published a report on the potential impact of BCIs, identifying questions we need to consider before we begin to think about realising the potential benefits:

- **Criminal liability:** What if a person commits a criminal act 'under the influence' of an implanted microchip? Who will be responsible? Was the person in control?
- **Employment:** Will BCIs be available only to those that can afford it, leading to a world characterised by neurotechnological discrimination where employees with implants will be paid more resulting from their ability to 'download' more desirable skills; or will we have no choice in the matter and wearing a BCI will be a condition of employment?
- **Data protection:** How can the user control what data leaves their BCI? If consent is relied upon, will it be valid? What can that data be used for? How do we ensure that data is kept secure – to date 'hacking' has only been thought of in a traditional computer context – but what about the brain?

Some of these questions will depend on how we realise the technology in the context of military, health and consumer applications. While Neuralink and Synchron are focussing on health, companies like Facebook have been considering how to use brain data for marketing ads for some years. This being the case, it's clear that regulation will be needed to ensure the safe deployment of the technology. The question then becomes when and how do we start?

How to regulate something that doesn't exist?

To date 39 countries have taken steps to consider regulation of neurotechnology by signing up to the OECD's non-binding recommendation on responsible innovation in neurotechnology. Adopted in 2019, the recommendation outlines nine principles that guide stakeholders through each stage of the innovation process (from research to commercialisation) with the goal of maximising the benefits of neurotechnology and minimising its risks. Examples of principles include:

- **Promote** responsible innovation in neurotechnology to address health challenges.
- **Anticipate** and monitor the potential unintended use and/or misuse of neurotechnology.

Although a good first step to get the conversation going (which is a success in itself), the breadth of principles and their non-binding nature, are significant limitations. Something

more robust with real 'bite' is needed to effectively regulate BCIs and this is where Chile is leading the pack.

The world led by Chile

Back in 2021, Chilean Senator Girardi understood the need to get ahead of the technology: *"we didn't regulate the big social media and internet platforms in time, and it cost us..."*
Shortly after this statement, Chile became the first country to implement legislation in the form of a constitutional amendment that enshrines the right of mental integrity of all citizens. The aim of the legislation is to protect mental privacy, free will, equal access to cognitive enhancement technologies and protection against algorithmic bias. The constitutional amendment was quickly followed up by a draft Chilean neuro-protection bill that seeks to underpin the new and broadly drafted constitutional rights, by giving personal brain data 'organ status' – meaning it cannot be bought or sold, trafficked or manipulated, and any data collection will require explicit 'opt-in' authorisation from the user.

EU – the first steps have been taken

In 2021, several EU countries went beyond the OECD's recommendation:

- France approved a bioethics law that protects the right to mental integrity;
- Spain adopted a 'digital rights charter' with a dedicated section on neuro rights; and
- the Italian Data Protection Authority commenced discussion on whether mental privacy is sufficiently covered under the country's privacy rights.

UK – let them innovate

Having signed the OCED's recommendations in 2019 and with the Law Society publishing a report in 2022, it's clear that neurotechnology is on the UK government's radar, but unlike Chile and its EU counterparts, the UK is taking a more commercial approach.
As the Law Society explains, there are risks if we regulate too late, but there are also risks if we regulate too early:

"It would be disastrous if progress in treating conditions that cause so much suffering and quite properly could be viewed as requiring urgent action, were unnecessarily slowed by too cautious a regulatory environment..."
This commercial approach to regulation is increasingly the norm in the UK, especially in areas like data protection and Artificial Intelligence. The UK's data protection authority (the ICO) is leading the way with its regulatory sandbox – a service that creates a space for technology companies to innovate in collaboration with the regulator, to push the limits of innovation within the boundaries of applicable regulation.

Whether neurotechnology is a good fit for the ICO's sandbox depends on how you view BCI technology. This problem has already been considered by the UK Parliament Office of Science and Technology – should neurotechnology be considered a 'personal data technology' regulated by the ICO, or a medical device regulated by the MHRA, or a consumer technology regulated by the CMA? Or maybe we need something new? In which case the UK's current approach seems sensible… at least for now.

Where does this leave us?

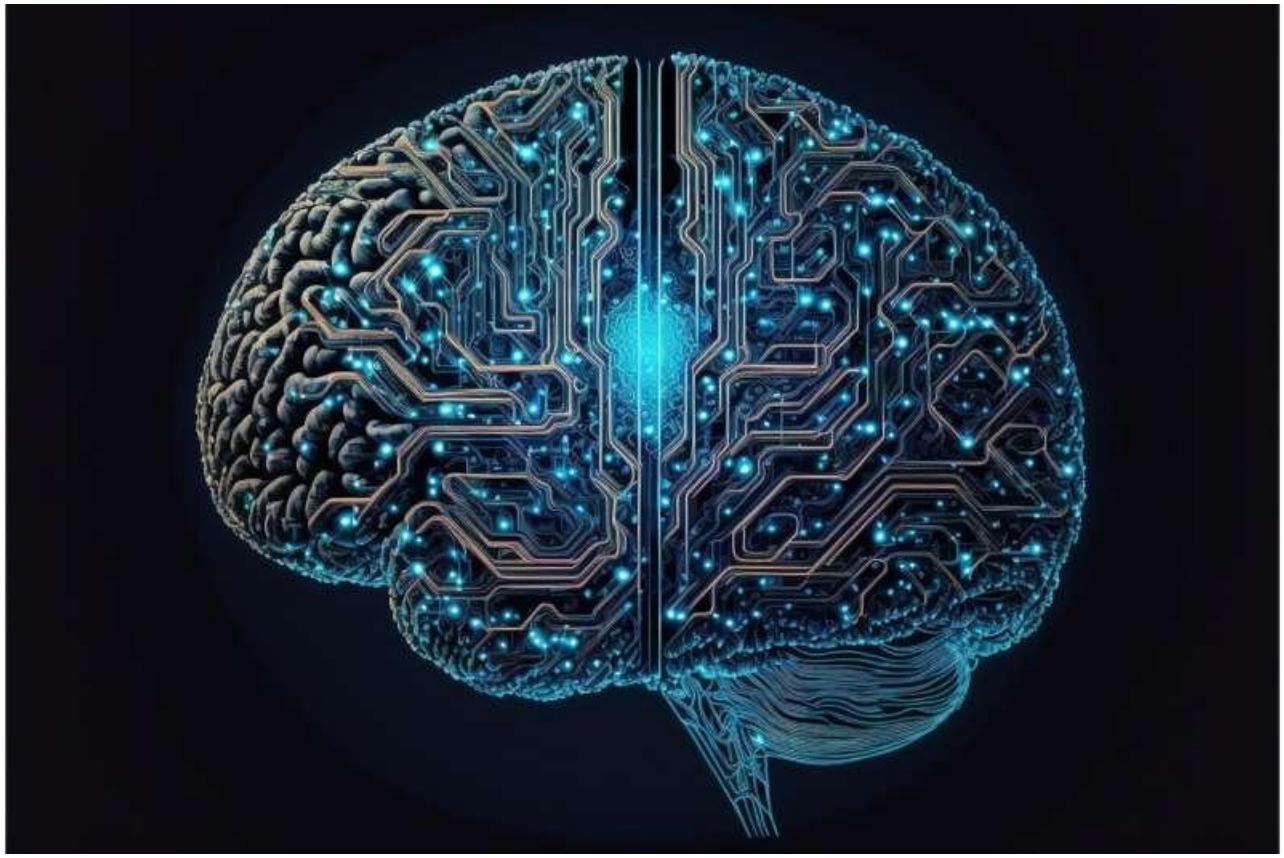
Neurotechnology is both exciting and potentially terrifying, BCIs offer clear benefits to humans in that they may be the key to managing or curing some of our most debilitating health conditions, and driving our functional advancements far beyond what seems possible today. But achieving those benefits comes with a ream of risks that need to be considered in order to safely realise the technology's full potential.

How we go about regulating neurotechnology is still up for debate. Each country seems to have very different views on how and when such regulation should come into being, the promising take away is that at least one of them has to be right…right?

FEBRUARY 25, 2025

New report explores merging Web 3.0 with AI technologies

by University of Surrey



Credit: Pixabay/CC0 Public Domain

The Surrey Academy for Blockchain and Metaverse Applications (SABMA), a pioneering institution within the University of Surrey, is proud to announce the release of its groundbreaking report: Web 3.0 Protocol-as-Platform: Vision and Framework for Decentralized Agentic Super Intelligence.

This comprehensive report, led by Professor Yu Xiong, Associate Vice-President (External Engagement) at the University of Surrey and Director of SABMA, presents a forward-thinking vision for the convergence of Web 3.0 and artificial intelligence (AI). It addresses current challenges in blockchain technology, such as fragmentation, scalability, and governance inefficiencies, and proposes an innovative Protocol-as-Platform (PaaP) approach. This framework emphasizes AI integration, cross-chain interoperability, and privacy-preserving mechanisms to foster a more decentralized and intelligent internet ecosystem.

The findings are published on the *SSRN* preprint server. Key insights from the report include:

- AI-driven smart contracts: The report introduces the concept of autonomous AI agents that can self-execute and adapt, enhancing efficiency and reducing human intervention in decentralized applications.
- Cross-chain inter-operability: A unified protocol layer is proposed to integrate multiple blockchain networks, facilitating seamless transactions and communication across platforms.
- Privacy-preserving mechanisms: Advanced cryptographic tools, such as Zero-Knowledge Proofs (ZKPs), are highlighted to ensure user data privacy and security within decentralized systems.
- Dynamic governance models: The report advocates for AI-driven decentralized autonomous organizations (DAOs) to optimize decision-making processes and enhance governance efficiency.

Professor Xiong commented, "Our goal with this report is to provide a roadmap for the next generation of decentralized applications and economies. By integrating AI and emphasizing modular, privacy-centric infrastructures, we aim to transition Web 3.0 from a speculative environment to a sustainable and user-friendly digital economy."

SABMA's next steps

Building upon the insights from the report, SABMA plans to:

- Launch educational initiatives: Develop intensive courses, workshops, and training programs to equip students and professionals with the skills needed to navigate and innovate in the evolving landscape of Web 3.0 and AI.
- Foster industry collaboration: Partner with leading technology firms and startups to pilot the proposed PaaP framework, facilitating real-world applications and feedback.
- Host conferences and lectures: Organize events featuring high-profile speakers from academia and industry to share insights and drive discussions on the future of decentralized intelligence.

SABMA, housed within the Surrey Business School, is dedicated to educating professionals in blockchain and metaverse applications through applied training courses and research initiatives. The Academy supports students in developing their knowledge and skills, fostering innovation and entrepreneurship in these emerging fields.

More information: Yu Xiong et al, Web 3.0 Protocol-as-Platform: Vision and Framework for Decentralized Agentic Super Intelligence, *SSRN* (2025). DOI: 10.2139/ssrn.5136445
Provided by University of Surrey

'Unbreakable' quantum communication closer to reality thanks to new, exceptionally bright photons

published August 26, 2024

Scientists build a new light source for quantum communications by combining existing technologies together to create a stronger and more robust quantum signal.

A future quantum internet could beam data at much longer distances than previously thought possible thanks to an exceptionally bright light source made by combining existing technologies in a new way. (Image credit: Pitris/Getty Images)

Scientists have created an "exceptionally bright" light source that can generate quantum-entangled photons (particles of light) which could be used to securely transmit data in a future high-speed quantum communications network.

A future quantum internet could transmit information using pairs of entangled photons — meaning the particles share information over time and space regardless of distance. Based on the weird laws of quantum mechanics, information encoded into these entangled photons can be transferred at high speeds while their "quantum coherence" — a state in which the particles are entangled — ensures the data cannot be intercepted.
But one of the key challenges in building a quantum internet has been that the strength of these photons can fade the further they travel; the light sources have not been bright enough. To build a successful quantum internet that can send data over vast distances, photons must be strong enough to prevent "decoherence" — where entanglement is lost

and the information they contain disappears. In research published 24 July in the journal eLight, scientists from Europe, Asia and South America created a new type of quantum signal source using existing technologies that achieves extremely high brightness.They achieved this by combining a photon dot emitter (a generator of single photons, or a particle of light) with a quantum resonator (a device to strengthen the quantum signature) to create the powerful new quantum signal.

What makes the recent research especially interesting is that the individual technologies have been independently proven in laboratories, but they had only been tested separately. This study is the first time they have been used in conjunction with each other.Researchers combined the photon dot emitter with a circular Bragg resonator (a reflector used to guide electromagnetic waves) on a piezoelectric actuator (a device that generates electricity when heat or stress is applied). Together they created an enhanced form of photon emitter, which can fine-tune the emitted photons for maximum polarized entanglement. This was controlled by using the piezoelectric actuator.

Photon pairs generated by the device had a high entanglement fidelity and extraction efficiency — meaning that each photon is bright enough to be useful and holds its "quantum signature" (a useful quantum property) well. It was previously hard to achieve both a useful level of brightness and a high entanglement fidelity at the same time, because each aspect required a different technology and these were difficult to combine in a scalable manner.

This is a significant step forward in developing practical quantum technologies, demonstrating how they can be combined together to create a more powerful and viable light source.

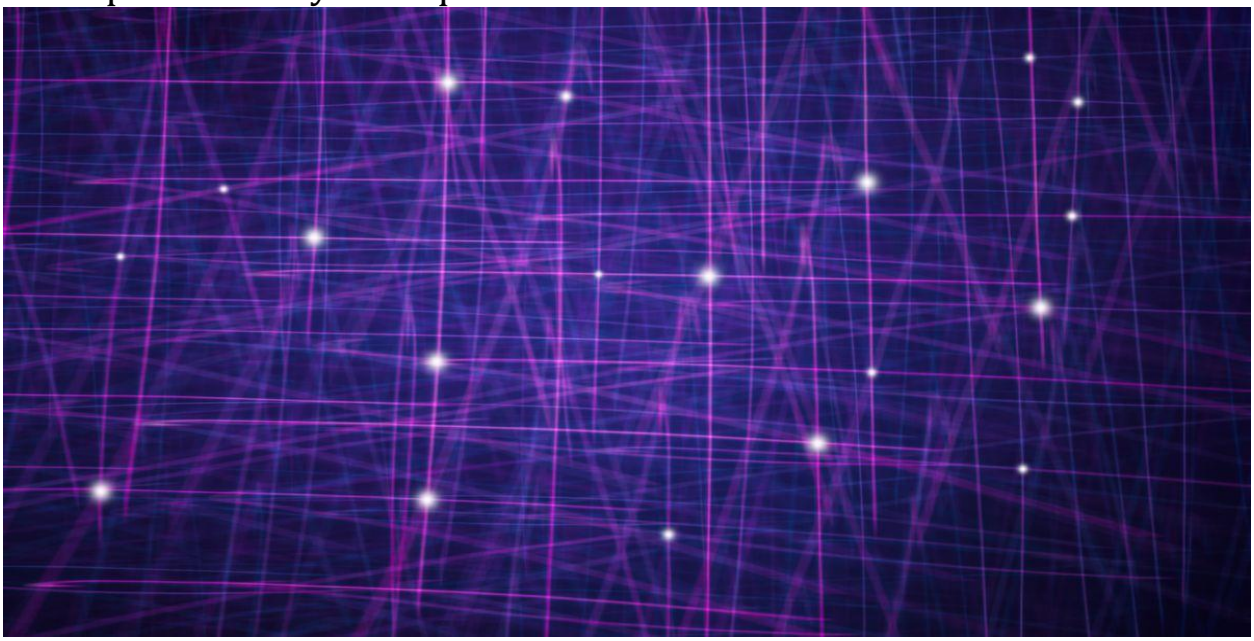
Unfortunately, we should not expect a quantum internet any time soon, as the various technologies remain in the experimental and development phase. Making the photon emitter used in the study also required toxic raw materials, including arsenic, which required specialist handling. There are also safety concerns around the use of gallium arsenide, which the photon dot emitter was made from. Fisher Scientific, a supplier of laboratory equipment and chemicals for scientific research, lists gallium arsenide as hazardous for several reasons, including its carcinogenic properties.
The safety concerns relating to the use of these materials could limit the scalability of the methodology outlined. Viable alternative materials may therefore need to be identified in generating bright, entangled photons for future quantum communications network

The next stage in the development process will be to integrate a diode-like structure onto the piezoelectric actuator. This would allow an electric field to be generated across the quantum dots, in order to counteract decoherence and therefore boost the degree of entanglement.

Although there are many further steps to take in developing a quantum internet, successfully combining a photon emitter and a resonator to achieve photons with high brightness and entanglement is nonetheless a significant step forward, the scientists said.

QUANTUM MEMORY

A new technique in quantum storage that operates at room temperature could pave the way for a quantum internet.



As well as being faster, quantum communications are inherently secure — while classical communications can be intercepted or manipulated. (Image credit: PM Images via Getty Images)

We're now one step closer to a "quantum internet" — an interconnected web of quantum computers — after scientists built a network of "quantum memories" at room temperature for the first time.

In their experiments, the scientists stored and retrieved two photonic qubits — qubits made from photons (or light particles) — at the quantum level, according to their paper published on Jan. 15 in the Nature journal, Quantum Information.
The breakthrough is significant because quantum memory is a foundational technology that will be a precursor to a quantum internet – the next generation of the World Wide Web.

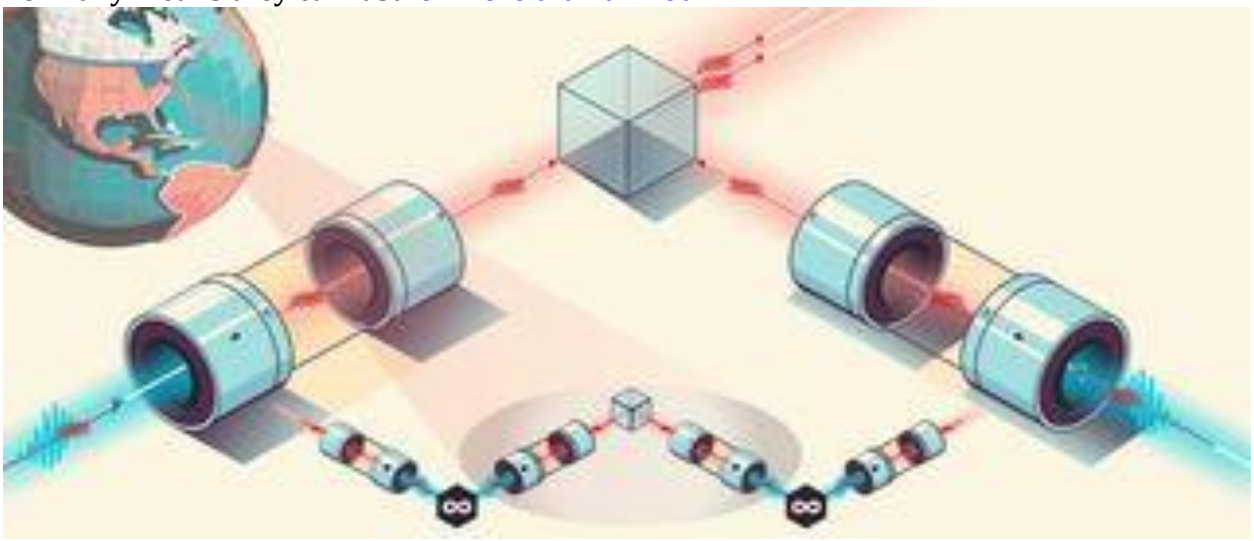
Quantum memory is the quantum version of binary computing memory. While data in classical computing is encoded in binary states of 1 or 0, quantum memory stores data as a quantum bit, or qubit, which can also be a superposition of 1 and 0. If observed, the superposition collapses and the qubit is as useful as a conventional bit.

Quantum computers with millions of qubits are expected to be vastly more powerful than today's fastest supercomputers — because entangled qubits (intrinsically linked over space and time) can make many more calculations simultaneously.

As the name implies, the quantum internet is an internet infrastructure that relies on the laws of quantum mechanics to transmit data between quantum computers. But we need quantum memory for a quantum network to function. Because qubits adopt a superposition of 1 and 0, rather than either binary state as in classical computing, they can store and transmit more information with far greater density than conventional networks.
"To get these fleets of quantum memories to work together at a quantum level, and in a room temperature state, is something that is essential for any quantum internet on any scale. To our knowledge, this feat has not been demonstrated before, and we expect to build on this research," said lead author Eden Figueroa, professor of physics and astronomy at Stony Brook University, in a statement.

Building a network for quantum computing

Quantum networks built in recent years have needed to be cooled to absolute zero to operate, which limits their usefulness. But scientists from Stony Brook University developed a method to store two separate photons and – most importantly – successfully retrieve their quantum signature. They achieved this at room temperature by storing photons in a rubidium gas.
This makes it more viable than previous experiments in designing and deploying a quantum internet in the future. However, they could only store the photons in this experiment for a fraction of a second, while storing qubits at cryogenic temperatures normally means they can last for more than an hour.



Quantum repeaters require two sources of entangled photon pairs separated by a distance — where one photon is sent towards a quantum memory store, and the other photon is sent in the opposite direction. (Image credit: Chase Wallace, Stony Brook University)

"The actual selling point of this was that they were able to take two independently stored photons, retrieve them at the same time, and interfere them," Daniel Oi, a professor in quantum physics at the University of Strathclyde, told Live Science. "You get what's called a HOM dip, or a Hong-Ou-Mandel dip, which is a characteristic quantum signature indicating that these two photons were identical."
As well as being faster, quantum communications are inherently secure — while classical communications can be intercepted or manipulated. This is because any attempts to

intercept and read information transmitted across the quantum network equates to observation — which would collapse the superposition of the qubits moving through the circuit.

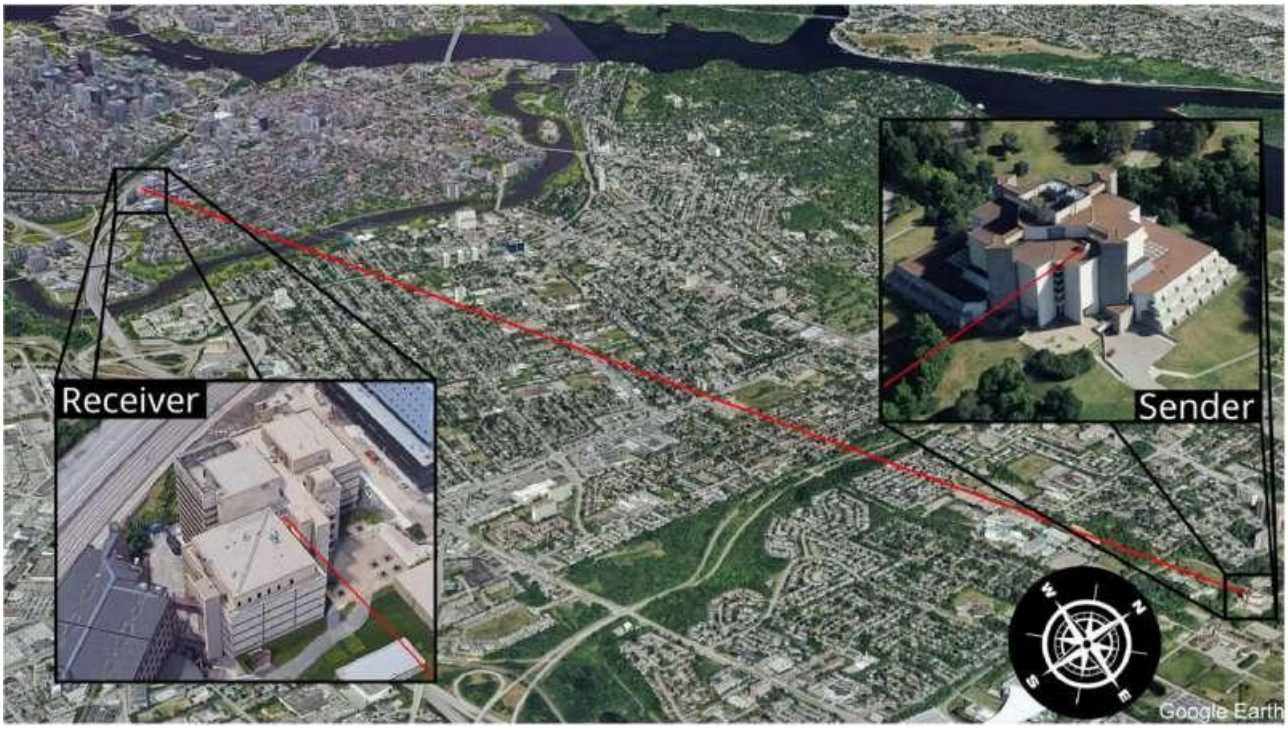
This is an active field of research and a race is underway to develop the technologies that will help us build a quantum internet. In 2022, researchers in Switzerland stored a single photon using a similar method. That same year, China transmitted signals using quantum entanglement between two memory devices located 12.5 kilometers apart.
The next stage is to develop a method for detecting when a quantum signal is ready to be retrieved, without destroying the properties of the signal through direct observation. Achieving this would pave the way for quantum repeaters, which are devices that can extend the range of a quantum signal. This would be a key precursor to a large-scale quantum internet.

- “One of the holy grails of quantum memories is ‘How do you detect that you’ve actually stored a photon, without destroying the quantum properties of that photon.

MARCH 4, 2025

AI and adaptive optics propel free-space quantum communication by solving atmospheric turbulence challenges

by University of Ottawa



Channel path. The path over which the turbulence data was collected from July 2023 to March 2024. The receiver is on the University of Ottawa campus, while the sender is on the Canadian National Research Council 5.4 km East-North-East. This configuration was chosen to minimize the background levels caused by the sunlight. Credit: *Optics Express* (2025). DOI: 10.1364/OE.546606

In the quest for ultra-secure, long-range quantum communication, two major challenges stand in the way: the unpredictable nature of atmospheric turbulence and the limitations of current optical wavefront correction techniques. Researchers at the University of Ottawa, under the supervision of Professor Ebrahim Karimi, the director of Nexus for Quantum Technologies, in collaboration with the National Research Council Canada (NRC) and the Max Planck Institute for the Science of Light (Germany), have made significant advances in overcoming both obstacles.

Their two latest breakthroughs—an AI-powered turbulence forecasting tool called TAROQQO and a high-speed Adaptive Optics (AO) system for correcting turbulence in quantum channels—represent a turning point in developing free-space quantum networks.

These advancements, published in *Optics Express* and *Communication Physics*, offer complementary solutions to the fundamental issue of atmospheric turbulence that distorts and diminishes photonic quantum states as they traverse through the air.

While TAROQQO facilitates real-time turbulence forecasting to optimize experimental conditions, the fast adaptive optics system actively rectifies turbulence-induced errors, ensuring dependable, high-dimensional quantum communication even under adverse conditions.

TAROQQO and AI-driven turbulence forecasting

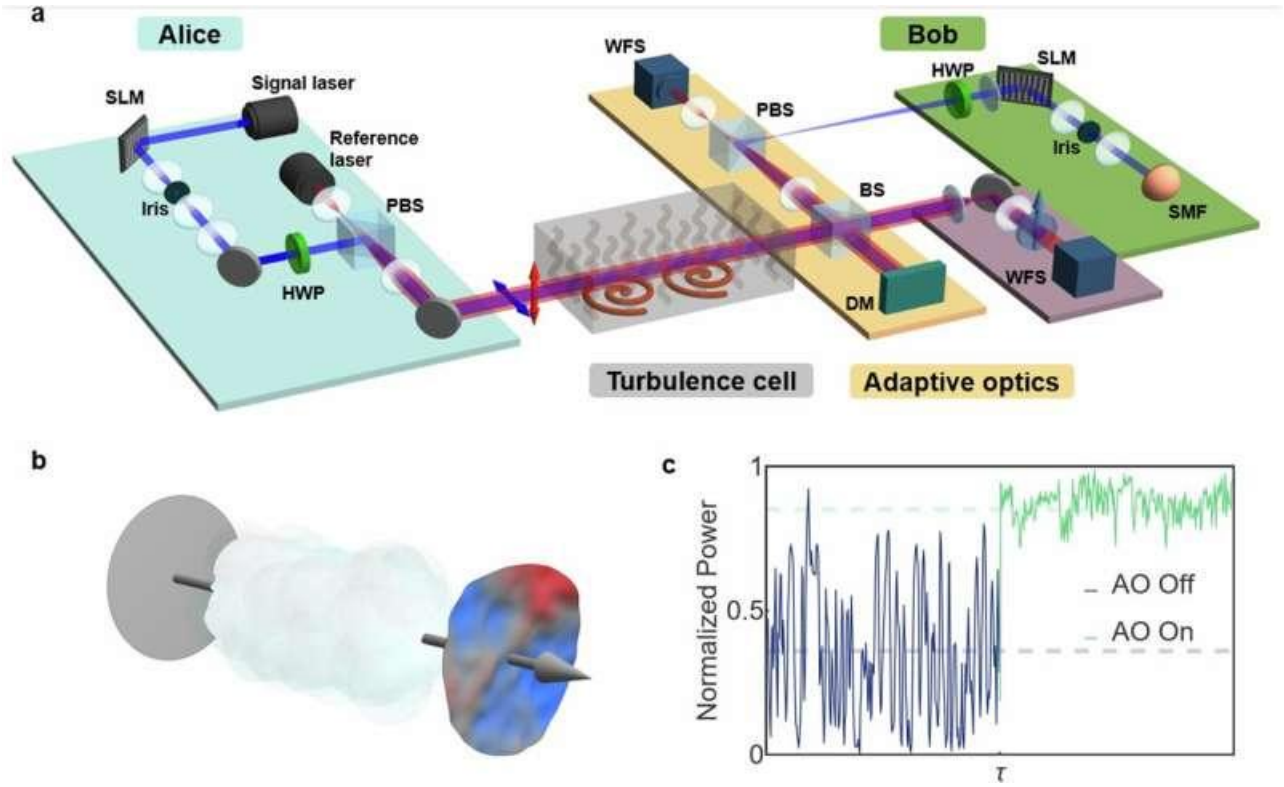
One key challenge in free-space quantum communication—particularly in satellite-based and intra-city networks—is the constant fluctuation of the atmosphere. This can unpredictably disrupt the quantum states of light used for secure communication. To address this, Ph.D. students Tareq Jaouni, Lukas Scarfe, and Dr. Francesco Di Colandrea developed TAROQQO, a turbulence prediction tool based on Recurrent Neural Networks (RNNs).

By employing real-time weather data—including humidity, solar radiation, temperature, pressure, and a turbulence parameter known as C_n^2—TAROQQO can accurately predict turbulence strength up to 12 hours in advance, offering a time resolution as precise as one minute. This enables researchers to anticipate atmospheric conditions and plan their quantum experiments at optimal times, thereby avoiding unnecessary losses and maximizing the efficiency of free-space quantum links.

Beyond simple forecasting, TAROQQO also allows scientists to simulate the effects of turbulence on different quantum experiments, helping optimize quantum network deployment strategies. The complete TAROQQO software is now publicly available on GitHub—TAROQQO, enabling the global scientific community to integrate turbulence forecasting into their own quantum research and communication networks.

"By enhancing efficiency, cutting costs, and ensuring improved resource allocation, TAROQQO will serve as an invaluable tool for experimental physicists," stated Dr. Francesco Di Colandrea.

While TAROQQO anticipates turbulence, a second breakthrough from the University of Ottawa team directly combats its effect on photonic quantum states in real-time.



High-dimensional quantum communication with adaptive optics through a turbulent channel. Credit: *Communications Physics* (2025). DOI: 10.1038/s42005-025-01986-6

Fighting turbulence with speed and precision

Even with turbulence forecasting, certain quantum communication scenarios—such as free-space links and satellite-based quantum channels—necessitate immediate correction of optical distortions. To achieve this, the research team has successfully implemented a rapid and accurate adaptive optics system to restore the photons' quantum state in real-time.

Quantum Key Distribution (QKD) is a cryptographic technique rooted in the principles of quantum mechanics, allowing two parties to securely generate a random encryption key while simultaneously detecting any potential eavesdropping. If an unauthorized entity attempts to intercept the transmission, the very act of measurement disturbs the quantum states, introducing noise and immediately revealing the presence of an intruder.

When conducting high-dimensional QKD (encryption beyond 0 and 1) in free space, atmospheric turbulence introduces noise that reduces efficiency and, in extreme circumstances, renders the channel unsecure since any noise is assigned to eavesdroppers.

The University of Ottawa researchers have now demonstrated that adaptive optics (AO) can correct these distortions in real time, restoring the channel's security and enabling high-

dimensional quantum information transfer. AO works by using a custom deformable mirror that can change its shape up to 3000 times per second to compensate for fast turbulence effects before the measurement of quantum signals is performed.

"In our controlled laboratory experiment, we simulated a turbulent free-space quantum channel to evaluate the effectiveness of our adaptive optics system. The results were striking," said Ph.D. student Lukas Scarfe. "Without adaptive optics, turbulence introduced errors that exceeded the security threshold, making quantum key distribution impossible. However, with adaptive optics enabled, we successfully restored the channel, performing high-dimensional QKD and encoding up to three bits per photon—significantly boosting the key generation rate."

These findings illustrate that adaptive optics presents a viable solution for practical quantum experiments and quantum networks, allowing secure communication even under extreme atmospheric conditions.

The University of Ottawa's pioneering efforts in turbulence prediction (TAROQQO) and real-time turbulence correction (AO for QKD) provide complementary solutions that, when combined, pave the way for robust and scalable free-space quantum communication. Indeed, TAROQQO enables pre-emptive scheduling of quantum communication sessions to minimize disruptions, and Adaptive Optics actively corrects real-time turbulence distortions, ensuring reliable quantum key distribution.

These breakthroughs are crucial for the next generation of ground-to-satellite, underwater and free-space quantum communications and the deployment of global-scale quantum networks.

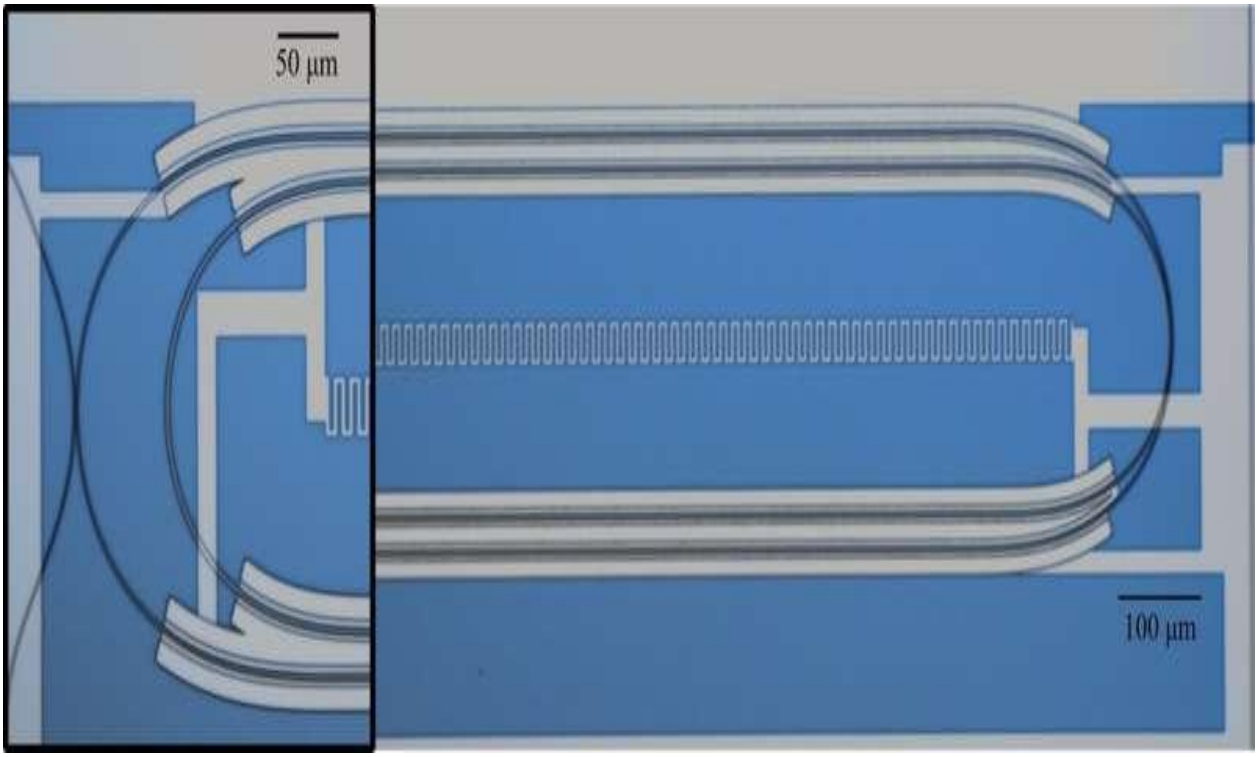
More information: Tareq Jaouni et al, Predicting atmospheric turbulence for secure quantum communications in free space, *Optics Express* (2025). DOI: 10.1364/OE.546606

Lukas Scarfe et al, Fast adaptive optics for high-dimensional quantum communications in turbulent channels, *Communications Physics* (2025). DOI: 10.1038/s42005-025-01986-6
Journal information: Communications Physics, Optics Express
Provided by University of Ottawa

APRIL 2, 2025

A router for photons: Transducer could enable superconducting quantum networks

by Harvard John A. Paulson School of Engineering and Applied Sciences



Optical micrograph of the microwave-optical quantum transducer. Credit: Lončar group / Harvard SEAS

Applied physicists at the Harvard John A. Paulson School of Engineering and Applied Sciences (SEAS) have created a photon router that could plug into quantum networks to create robust optical interfaces for noise-sensitive microwave quantum computers.

The breakthrough is a crucial step toward someday realizing modular, distributed quantum computing networks that leverage existing telecommunications infrastructure. Comprising millions of miles of optical fiber, today's fiber-optic networks send information between computing clusters as pulses of light, or photons, all around the world in the blink of an eye.

Led by Marko Lončar, the Tiantsai Lin Professor of Electrical Engineering and Applied Physics at SEAS, the team has created a microwave-optical quantum transducer, a device designed for quantum processing systems that use superconducting microwave qubits as their smallest units of operation (analogous to the 1s and 0s of classical bits).

The research is published in *Nature Physics*.

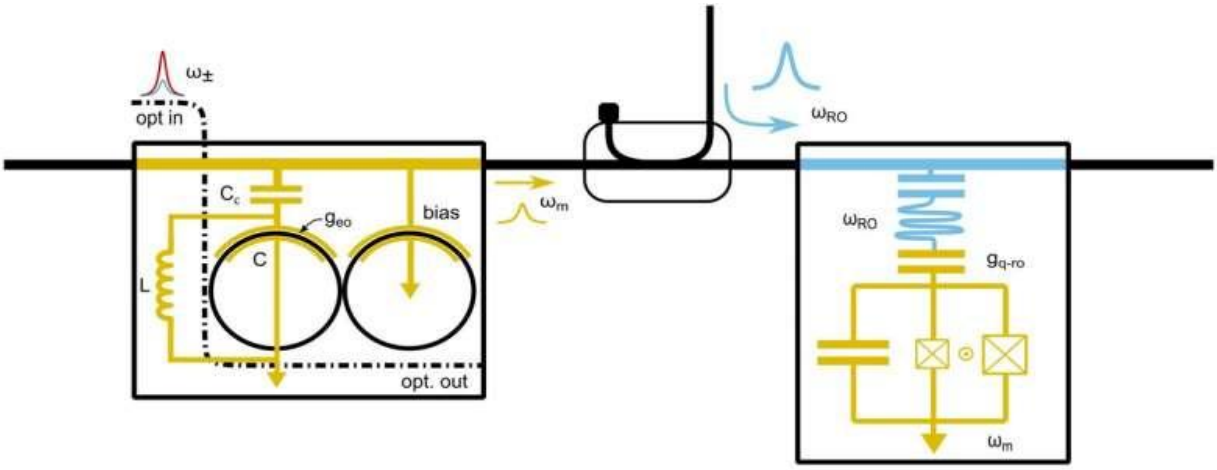
Effectively a router for photons, the transducer bridges the large energy gap between microwave and optical photons, thus enabling control of microwave qubits with optical signals generated many miles away. The device is the first of its kind to demonstrate control of a superconducting qubit using only light.

Paper first author and graduate student Hana Warner said the transducer offers a way to tap the power of optics when dreaming up quantum networks.

"The realization of these systems is still a ways out, but in order to get there, we need to figure out practical ways to scale and interface with the different components," Warner said.

"Optical photons are one of the best ways you can do that, because they're very good carriers of information, with low loss, and high bandwidth."

Superconducting qubits, which are nanofabricated circuits engineered for different energy states, are an emerging quantum computing platform due to their scalability, compatibility with existing manufacturing processes, and ability to maintain quantum superposition long enough to perform calculations.



Transducer-driven superconducting qubit scheme. Credit: Lončar group / Harvard SEAS

But one of the major bottlenecks to deploying superconducting microwave qubit platforms is the extremely low temperatures at which they must operate, necessitating large cooling systems called dilution refrigerators.

Since future quantum computing will require millions of qubits to operate, scaling these systems only on microwave-frequency signals is challenging. The solution lies in using microwave qubits to do the quantum operations, but to use optical photons as efficient and scalable interfaces.

That's where the transducer comes in.

The Harvard team's 2-millimeter optical device resembles a paper clip and sits on a chip that's about 2 centimeters in length. It works by linking a microwave resonator with two

optical resonators, allowing back-and-forth exchange of energy enabled by the properties of their base material, lithium niobate. The team leveraged this exchange to eliminate the need for bulky, hot microwave cables for controlling qubit states.

The same devices used for control could be used for qubit state readout, or for forming direct links to convert finicky quantum information into sturdy packets of light between quantum computing nodes. The breakthrough brings us closer to a world with superconducting quantum processors connected by low-loss, high-powered optical networks.

"The next step for our transducer could be reliable generation and distribution of entanglement between microwave qubits using light," Lončar said.

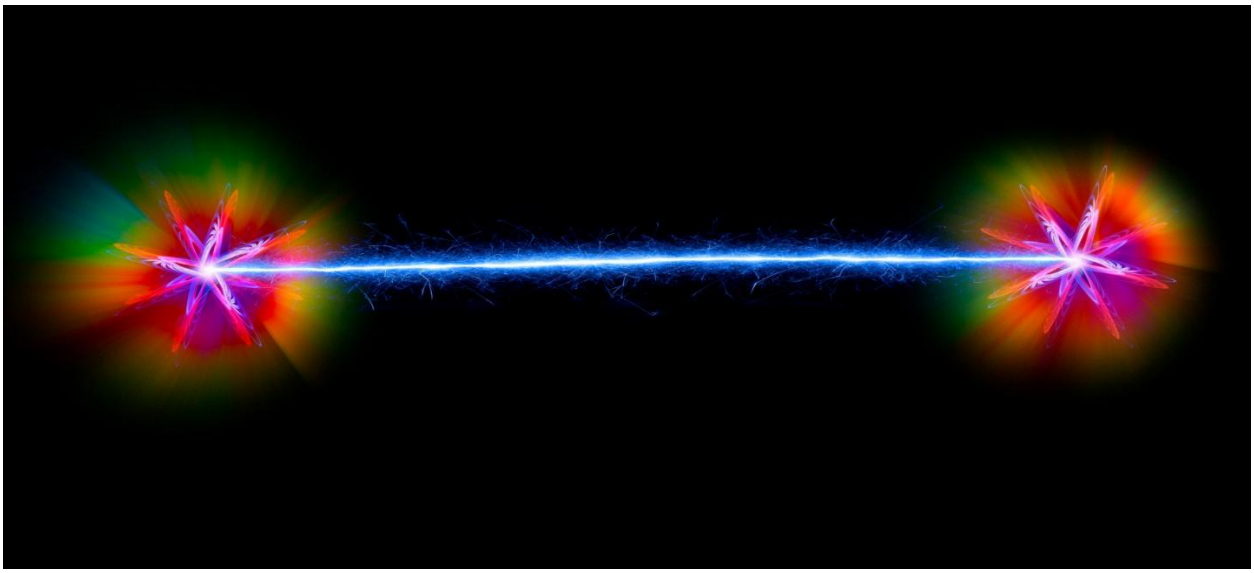
The Harvard team combined their expertise in optical systems with collaborators at Rigetti Computing, who provided the aluminum-on-silicon superconducting qubit platforms on which the researchers tested their transducer and mapped out different experiments. Other collaborators were from the University of Chicago and Massachusetts Institute of Technology.

Fabrication of the chips was performed at Harvard's Center for Nanoscale Systems, a member of the National Nanotechnology Coordinated Infrastructure Network.

More information: Coherent control of a superconducting qubit using light, *Nature Physics* (2025). DOI: 10.1038/s41567-025-02812-0
Journal information: Nature Physics
Provided by Harvard John A. Paulson School of Engineering and Applied Sciences

Scientists discover simpler way to achieve Einstein's 'spooky action at a distance' thanks to AI breakthrough — bringing quantum internet closer to reality published March 5, 2025

AI has helped physicists discover a simpler way of achieving quantum entanglement. This finding could make it easier to develop quantum communication technologies.



Scientists have used AI to discover an easier method to form quantum entanglement between subatomic particles, paving the way for simpler quantum technologies.

When particles such as photons become entangled, they can share quantum properties — including information — regardless of the distance between them. This phenomenon is important in quantum physics and is one of the features that makes quantum computers so powerful.
But the bonds of quantum entanglement have typically proven challenging for scientists to form. This is because it requires the preparation of two separate entangled pairs, then measuring the strength of entanglement — called a Bell-state measurement — on a photon from each of the pairs.

These measurements cause the quantum system to collapse and leave the two unmeasured photons entangled, despite them never having directly interacted with one another. This process of "entanglement swapping" could be used for quantum teleportation.

In a new study, published Dec. 2, 2024 in the journal Physical Review Letters, scientists used PyTheus, an AI tool that has been specifically created for designing quantum-optic experiments. The authors of the paper initially set out to reproduce established protocols for entanglement swapping in quantum communications. However, the AI tool kept producing a much simpler method to achieve quantum entanglement of photons.

"The authors were able to train a neural network on a set of complex data that describes how you set up this kind of experiment in many different conditions, and the network actually learned the physics behind it," Sofia Vallecorsa, a research physicist for the quantum technology initiative at CERN, who was not involved in the new research, told Live Science.

Tapping into AI to simplify quantum entanglement

The AI tool proposed that entanglement could emerge because the path of photons were indistinguishable: when there are several possible sources the photons could have come from, and if their origins become indistinguishable from one another, then entanglement can be produced between them when none existed before.

Although the scientists were initially skeptical of the results, the tool kept returning the same solution so they tested the theory. By adjusting the photon sources and ensuring they were indistinguishable, the physicists created conditions where detecting photons at certain paths guaranteed that two others emerged entangled.

This breakthrough in quantum physics has simplified the process by which quantum entanglement can be formed. In future, it could have implications for the quantum networks used for secure messaging, making these technologies much more feasible.

"The more we can rely on simple technology, the more we can increase the range of applications," Vallecorsa said. "The possibility to build more complex networks, that could branch out in different geometries, could have a big impact with respect to the single end-to-end case."

Whether it is practical to scale the technology into a commercially viable process remains to be seen, however, as environmental noise and device imperfections could cause instability in the quantum system.

The new study has also provided a convincing argument for the use of AI as a research tool by physicists. "We are looking more into introducing AI, but there is still a little bit of scepticism, mostly due to what the role of the physicist is going to be once we start going that way," Vallecorsa said. "It is an opportunity for getting a very interesting result and shows in a very compelling way how this can be a tool that physicists use."

Quantum internet breakthrough after 'quantum data' transmitted through standard fiber optic cable for 1st time June 7, 2024

The study used a specialized photon source to transmit, store and retrieve quantum data, a major component of quantum data transmission.

A new quantum computing study claims that a recent finding in the production, storage and retrieval of "quantum data" has brought us one step closer to the quantum internet.

Currently, quantum information is unstable over long distances and quantum bits, or qubits — the carriers of quantum information — are easily lost or fragmented during transmission.

Classical computer bits are transmitted today as pulses of light through fiber optic cables using devices called "repeaters" to amplify signals across the length of the network. To transmit qubits over longer distances the way classical computer bits are transmitted today we need similar devices that can store and retransmit quantum states across the whole network, ensuring signal fidelity no matter how far the data has to go.

These quantum memory devices could receive, store and retransmit qubit states. The new study, conducted at Imperial College London, the University of Southampton, and the Universities of Stuttgart and Wurzburg in Germany, claims to have achieved this using standard fiber optic cables for the first time. The findings were published April 12 in the journal Scientific Advances.

All in the photon source

The researchers stored and retrieved photons — one of the potential carriers of quantum information — using a new and potentially much more efficient method.

"There are two main types of single photon sources,a process called non-linear optical frequency conversion and those based on single emitters," Sarah Thomas, professor of physics at Imperial College, London, told Live Science. "It's been demonstrated many times before that we can store photons from nonlinear optics in a quantum memory because you can engineer the source and memory to match. We used a particular single emitter called a quantum dot, which is a nanocrystal of semiconductors."
Thomas said that using nonlinear optics is less reliable — a pair of usable photons isn't produced every time, whereas a single emitter quantum dot produces them at a higher rate.

The next challenge is that the efficiency of the interface between quantum memory devices depends on matching both the wavelength and bandwidth. Discrepancies here make storage and retrieval too inefficient, but the study finally bridged the gap.

"We did it by using a high-bandwidth, low-noise quantum memory, fabricating the photon source at a very specific wavelength to match our quantum memory," Thomas said. "We were also able to do it at a wavelength where the loss in optical fiber is the lowest, which will be key in the future for building quantum networks."

Building on past work

But this is not the only recent advance in quantum computing and the quantum internet. In February, Live Science reported on a related breakthrough at Stony Brook University. Quantum network models are more stable at extremely low temperatures, which limits their real-world applications, but the study achieved a stable connection at room temperature, which puts it within reach of real-world use.

The Imperial study builds on that success thanks to the aligned wavelengths between transmitter and receiver.

"The Stony Brook study used photons at 795 nm [nanometers] and showed interference of two photons after storage and retrieval," Mark Saffman, chief scientist for quantum information at quantum-enabled products company Infleqtion told Live Science. "The Imperial study used a photon at 1529 nm (which is the standard telecom wavelength) and stored and retrieved it, but didn't show interference. The storage and retrieval of telecom wavelength is important for low-loss fiber transmission. Both studies advance different aspects of what's needed for a quantum network."

Michael Hasse, a cybersecurity expert (one of the areas where quantum networks will have the most impact) told Live Science that the Imperial study describes a method whereas the earlier study describes a mechanism necessary for that method to work.

"The Imperial work is about a means of establishing long-distance communication using repeaters," he said. "Quantum entanglement allows communications to be far apart in theory, but in reality it's easier when they're closer together. The Stony Brook study refers to the storage of quantum information at room temperature, which is necessary for cost-effective implementation of repeaters."

'Quantum memory breakthrough' may lead to a quantum internet

February 26, 2024

A new technique in quantum storage that operates at room temperature could pave the way for a quantum internet.

As well as being faster, quantum communications are inherently secure — while classical communications can be intercepted or manipulated. (Image credit: PM Images via Getty Images)

We're now one step closer to a "quantum internet" — an interconnected web of quantum computers — after scientists built a network of "quantum memories" at room temperature for the first time.

In their experiments, the scientists stored and retrieved two photonic qubits — qubits made from photons (or light particles) — at the quantum level, according to their paper published on Jan. 15 in the Nature journal, Quantum Information.
The breakthrough is significant because quantum memory is a foundational technology that will be a precursor to a quantum internet – the next generation of the World Wide Web.

Quantum memory is the quantum version of binary computing memory. While data in classical computing is encoded in binary states of 1 or 0, quantum memory stores data as a quantum bit, or qubit, which can also be a superposition of 1 and 0. If observed, the superposition collapses and the qubit is as useful as a conventional bit.

Quantum computers with millions of qubits are expected to be vastly more powerful than today's fastest supercomputers — because entangled qubits (intrinsically linked over space and time) can make many more calculations simultaneously.

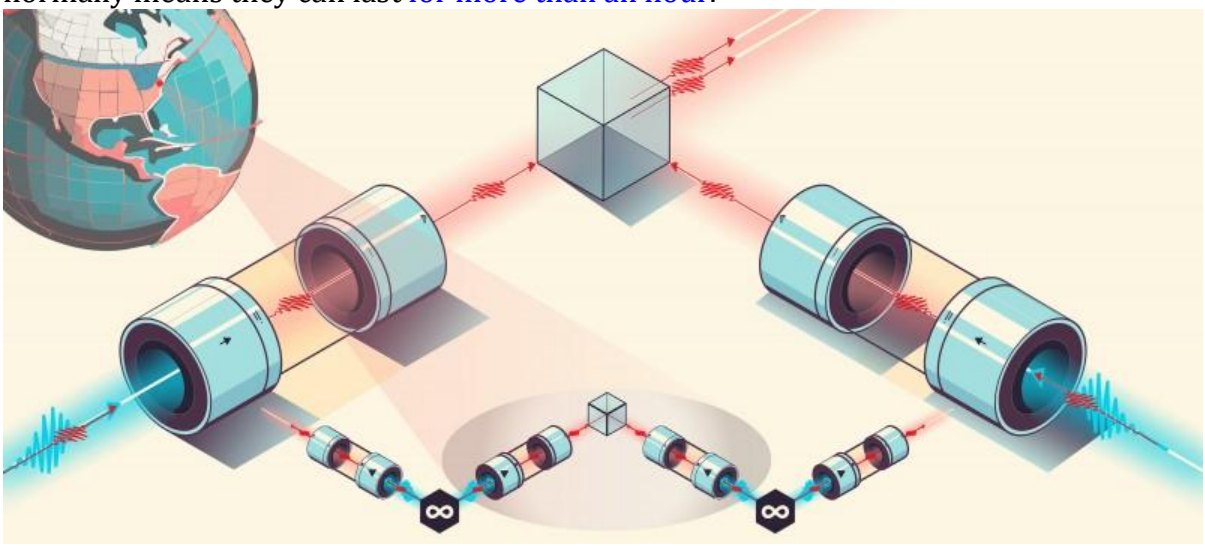
As the name implies, the quantum internet is an internet infrastructure that relies on the laws of quantum mechanics to transmit data between quantum computers. But we need quantum memory for a quantum network to function. Because qubits adopt a superposition of 1 and 0, rather than either binary state as in classical computing, they can store and transmit more information with far greater density than conventional networks.
“To get these fleets of quantum memories to work together at a quantum level, and in a room temperature state, is something that is essential for any quantum internet on any scale. To our knowledge, this feat has not been demonstrated before, and we expect to build on this research,” said lead author Eden Figueroa, professor of physics and astronomy at Stony Brook University, in a statement.

Building a network for quantum computing

Quantum networks built in recent years have needed to be cooled to absolute zero to operate, which limits their usefulness. But scientists from Stony Brook University

developed a method to store two separate photons and – most importantly – successfully retrieve their quantum signature. They achieved this at room temperature by storing photons in a rubidium gas.

This makes it more viable than previous experiments in designing and deploying a quantum internet in the future. However, they could only store the photons in this experiment for a fraction of a second, while storing qubits at cryogenic temperatures normally means they can last for more than an hour.



Quantum repeaters require two sources of entangled photon pairs separated by a distance — where one photon is sent towards a quantum memory store, and the other photon is sent in the opposite direction. (Image credit: Chase Wallace, Stony Brook University)

"The actual selling point of this was that they were able to take two independently stored photons, retrieve them at the same time, and interfere them," Daniel Oi, a professor in quantum physics at the University of Strathclyde, told Live Science. "You get what's called a HOM dip, or a Hong-Ou-Mandel dip, which is a characteristic quantum signature indicating that these two photons were identical."

As well as being faster, quantum communications are inherently secure — while classical communications can be intercepted or manipulated. This is because any attempts to intercept and read information transmitted across the quantum network equates to observation — which would collapse the superposition of the qubits moving through the circuit.

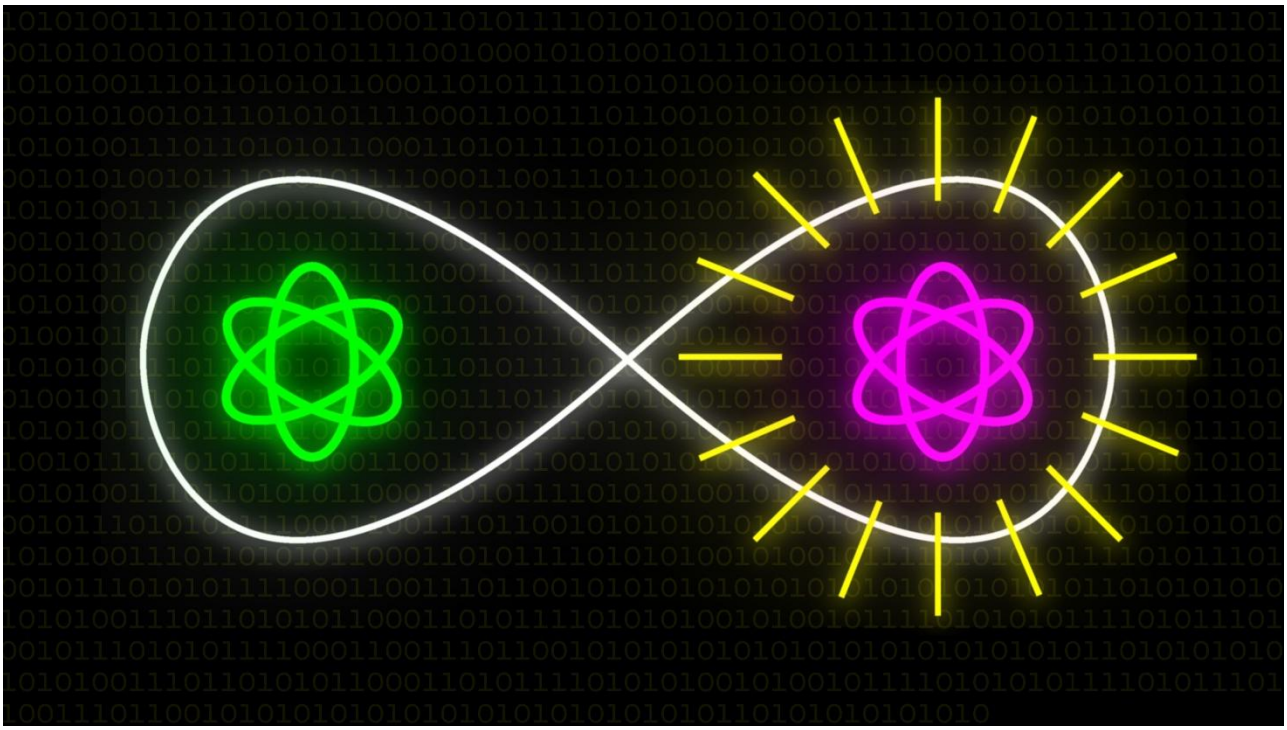
This is an active field of research and a race is underway to develop the technologies that will help us build a quantum internet. In 2022, researchers in Switzerland stored a single photon using a similar method. That same year, China transmitted signals using quantum entanglement between two memory devices located 12.5 kilometers apart.

The next stage is to develop a method for detecting when a quantum signal is ready to be retrieved, without destroying the properties of the signal through direct observation. Achieving this would pave the way for quantum repeaters, which are devices that can extend the range of a quantum signal. This would be a key precursor to a large-scale quantum internet.

“One of the holy grails of quantum memories is ‘How do you detect that you’ve actually stored a photon, without destroying the quantum properties of that photon, and do it in a way that is efficient and reliable?’,” said Oi.

Explainer: What is quantum communication?

Researchers and companies are creating ultra-secure communication networks that could form the basis of a quantum internet. This is how it works.



This is the second in a series of explainers on quantum technology. The other two are on quantum computing and post-quantum cryptography.

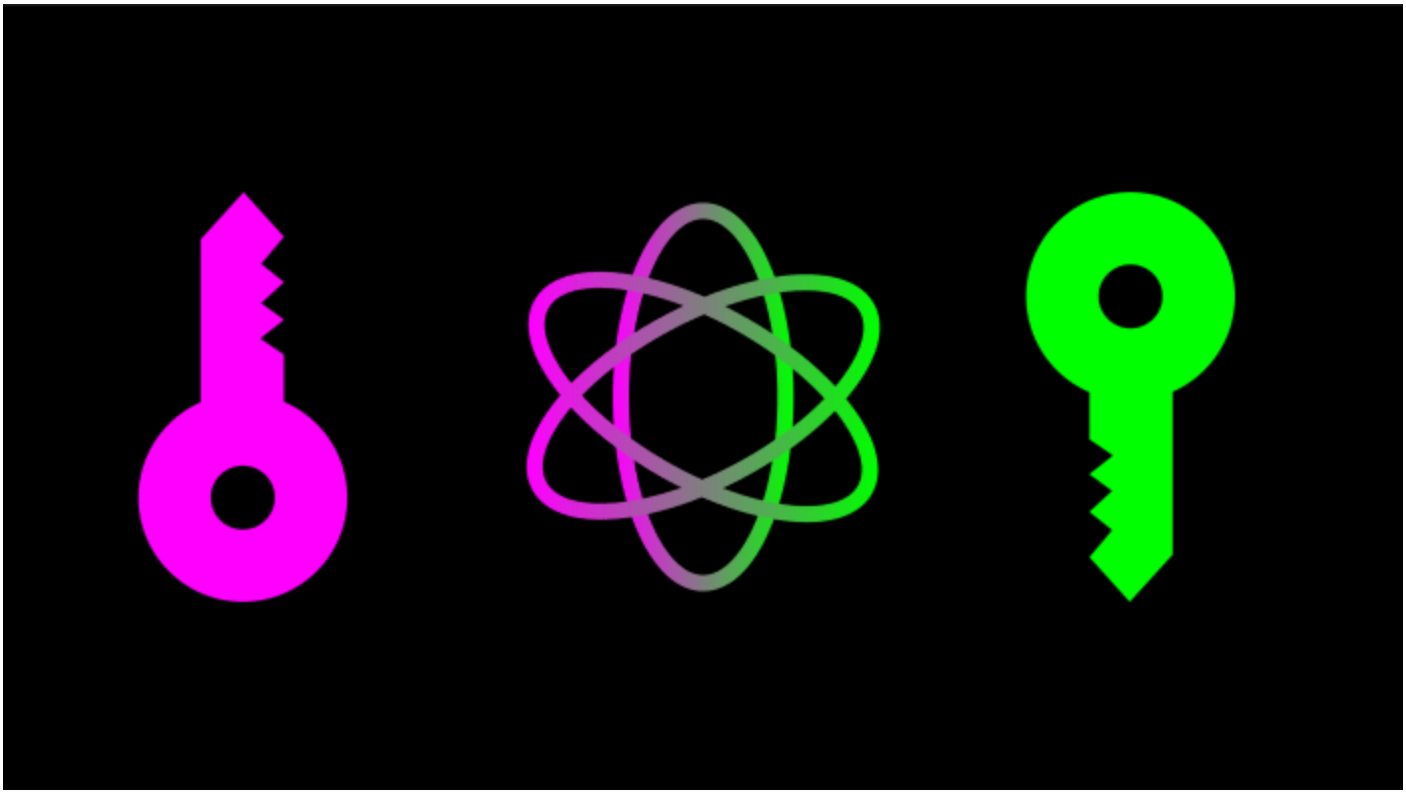
Barely a week goes by without reports of some new mega-hack that’s exposed huge amounts of sensitive information, from people’s credit card details and health records to companies’ valuable intellectual property. The threat posed by cyberattacks is forcing governments, militaries, and businesses to explore more secure ways of transmitting information.

Today, sensitive data is typically encrypted and then sent across fiber-optic cables and other channels together with the digital “keys” needed to decode the information. The data and the keys are sent as classical bits—a stream of electrical or optical pulses representing *1*s and *0*s. And that makes them vulnerable. Smart hackers can read and copy bits in transit without leaving a trace.

Quantum communication takes advantage of the laws of quantum physics to protect data. These laws allow particles—typically photons of light for transmitting data along optical cables—to take on a state of superposition, which means they can represent multiple combinations of *1* and *0* simultaneously. The particles are known as quantum bits, or qubits.

The beauty of qubits from a cybersecurity perspective is that if a hacker tries to observe them in transit, their super-fragile quantum state "collapses" to either *1* or *0*. This means a hacker can't tamper with the qubits without leaving behind a telltale sign of the activity.

Some companies have taken advantage of this property to create networks for transmitting highly sensitive data based on a process called quantum key distribution, or QKD. In theory, at least, these networks are ultra-secure.



What is quantum key distribution?

QKD involves sending encrypted data as classical bits over networks, while the keys to decrypt the information are encoded and transmitted in a quantum state using qubits.

Various approaches, or protocols, have been developed for implementing QKD. A widely used one known as BB84 works like this. Imagine two people, Alice and Bob. Alice wants to send data securely to Bob. To do so, she creates an encryption key in the form of qubits whose polarization states represent the individual bit values of the key.

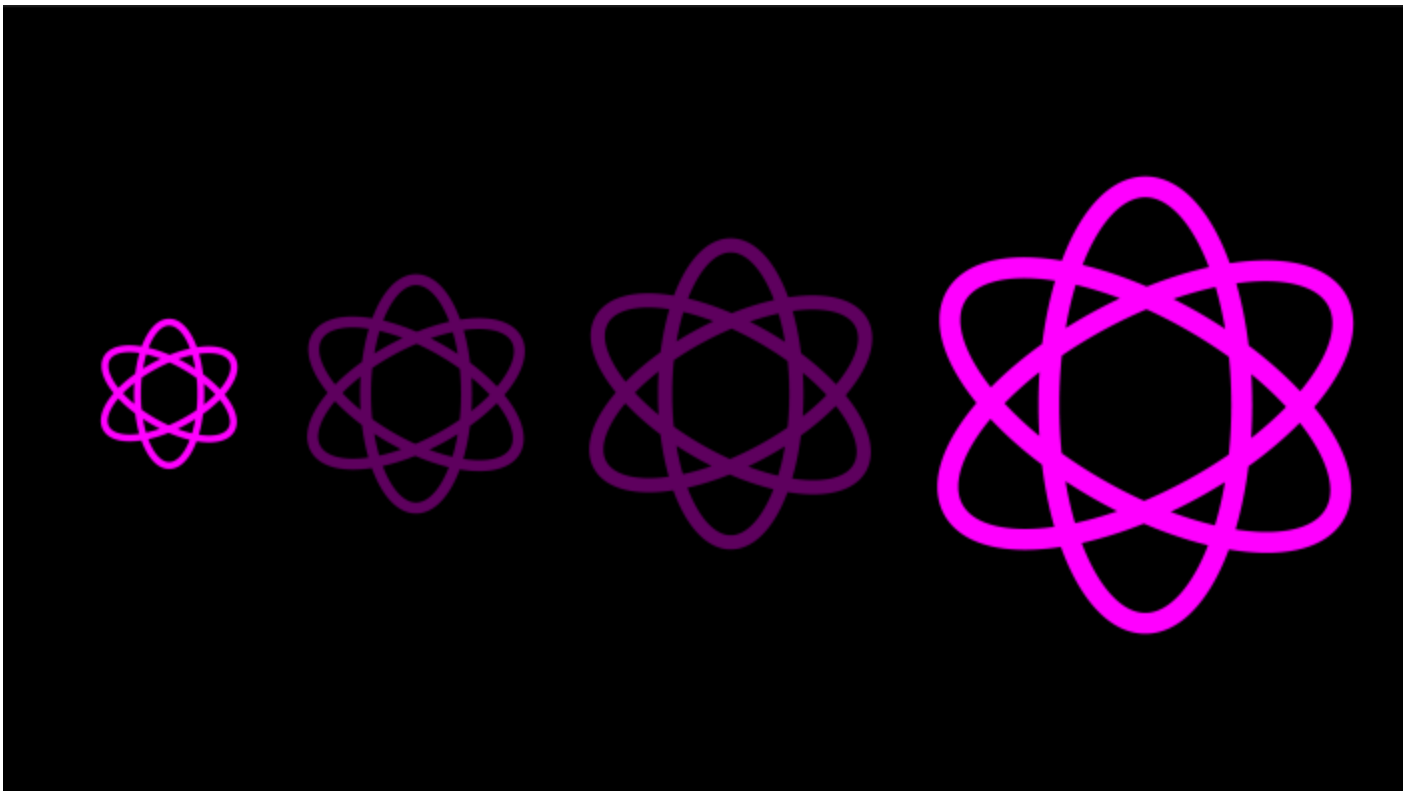
The qubits can be sent to Bob through a fiber-optic cable. By comparing measurements of the state of a fraction of these qubits—a process known as “key sifting”—Alice and Bob can establish that they hold the same key.

As the qubits travel to their destination, the fragile quantum state of some of them will collapse because of decoherence. To account for this, Alice and Bob next run through a process known as “key distillation,” which involves calculating whether the error rate is high enough to suggest that a hacker has tried to intercept the key.

If it is, they ditch the suspect key and keep generating new ones until they are confident that they share a secure key. Alice can then use hers to encrypt data and send it in classical bits to Bob, who uses his key to decode the information.

We’re already starting to see more QKD networks emerge. The longest is in China, which boasts a 2,032-kilometer (1,263-mile) ground link between Beijing and Shanghai. Banks and other financial companies are already using it to transmit data. In the US, a startup called Quantum Xchange has struck a deal giving it access to 500 miles (805 kilometers) of fiber-optic cable running along the East Coast to create a QKD network. The initial leg will link Manhattan with New Jersey, where many banks have large data centers.

Although QKD is relatively secure, it would be even safer if it could count on quantum repeaters.



What is a quantum repeater?

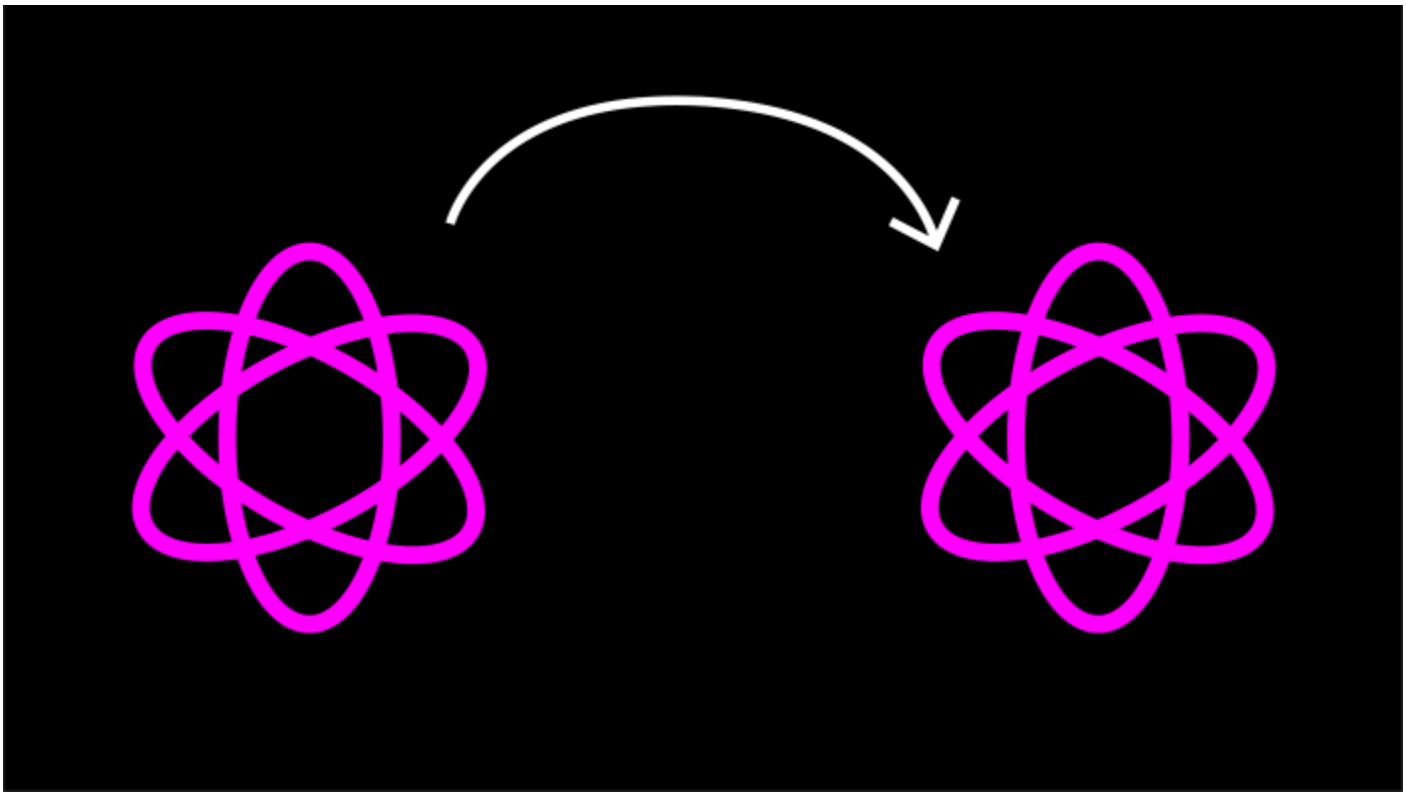
Materials in cables can absorb photons, which means they can typically travel for no more than a few tens of kilometers. In a classical network, repeaters at various points along a cable are used to amplify the signal to compensate for this.

QKD networks have come up with a similar solution, creating “trusted nodes” at various points. The Beijing-to-Shanghai network has 32 of them, for instance. At these waystations, quantum keys are decrypted into bits and then reencrypted in a fresh quantum state for their journey to the next node. But this means trusted nodes can’t really be trusted: a hacker who breached the nodes’ security could copy the bits undetected and thus acquire a key, as could a company or government running the nodes.

Ideally, we need quantum repeaters, or waystations with quantum processors in them that would allow encryption keys to remain in quantum form as they are amplified and sent over long distances. Researchers have demonstrated it’s possible in principle to build such repeaters, but they haven’t yet been able to produce a working prototype.

There’s another issue with QKD. The underlying data is still transmitted as encrypted bits across conventional networks. This means a hacker who breached a network’s defenses could copy the bits undetected, and then use powerful computers to try to crack the key used to encrypt them.

The most powerful encryption algorithms are pretty robust, but the risk is big enough to spur some researchers to work on an alternative approach known as quantum teleportation.



What is quantum teleportation?

This may sound like science fiction, but it's a real method that involves transmitting data wholly in quantum form. The approach relies on a quantum phenomenon known as entanglement.

Quantum teleportation works by creating pairs of entangled photons and then sending one of each pair to the sender of data and the other to a recipient. When Alice receives her entangled photon, she lets it interact with a "memory qubit" that holds the data she wants to transmit to Bob. This interaction changes the state of her photon, and because it is entangled with Bob's, the interaction instantaneously changes the state of his photon too.

In effect, this "teleports" the data in Alice's memory qubit from her photon to Bob's. The graphic below lays out the process in a little more detail:

How quantum teleportation works

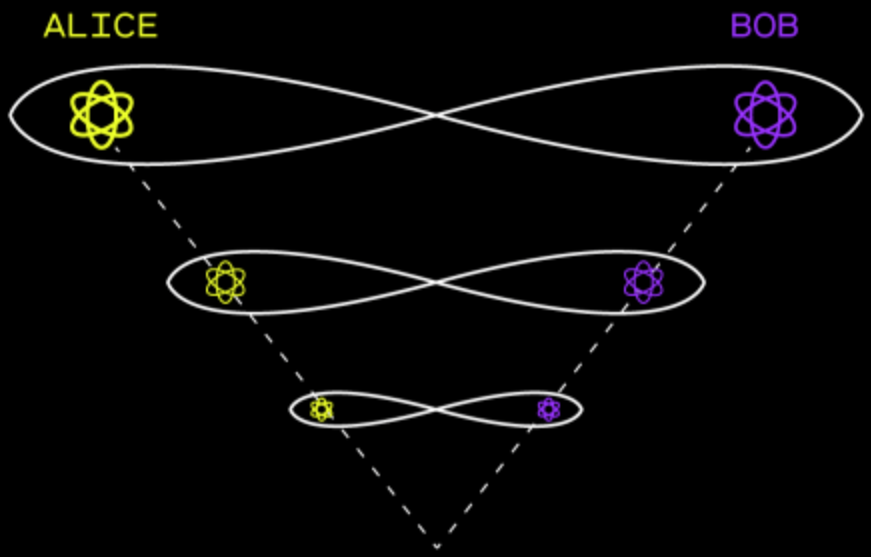


Figure 1.
Alice and Bob receive pairs of entangled qubits in the form of photons.

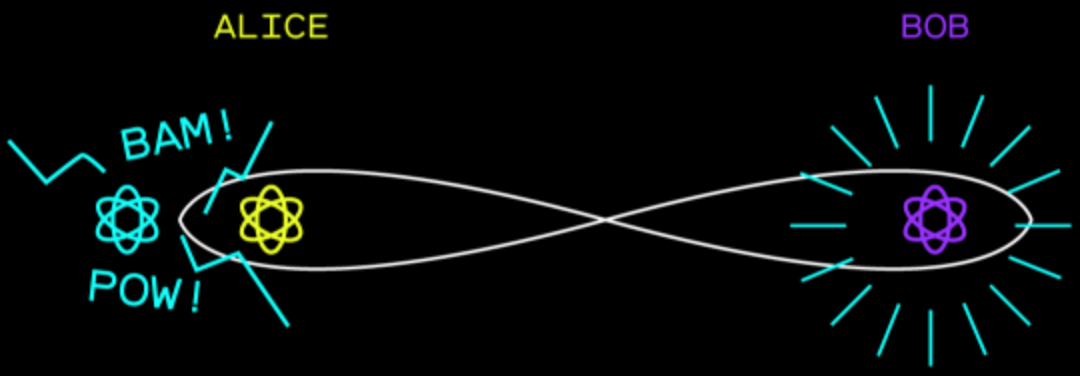
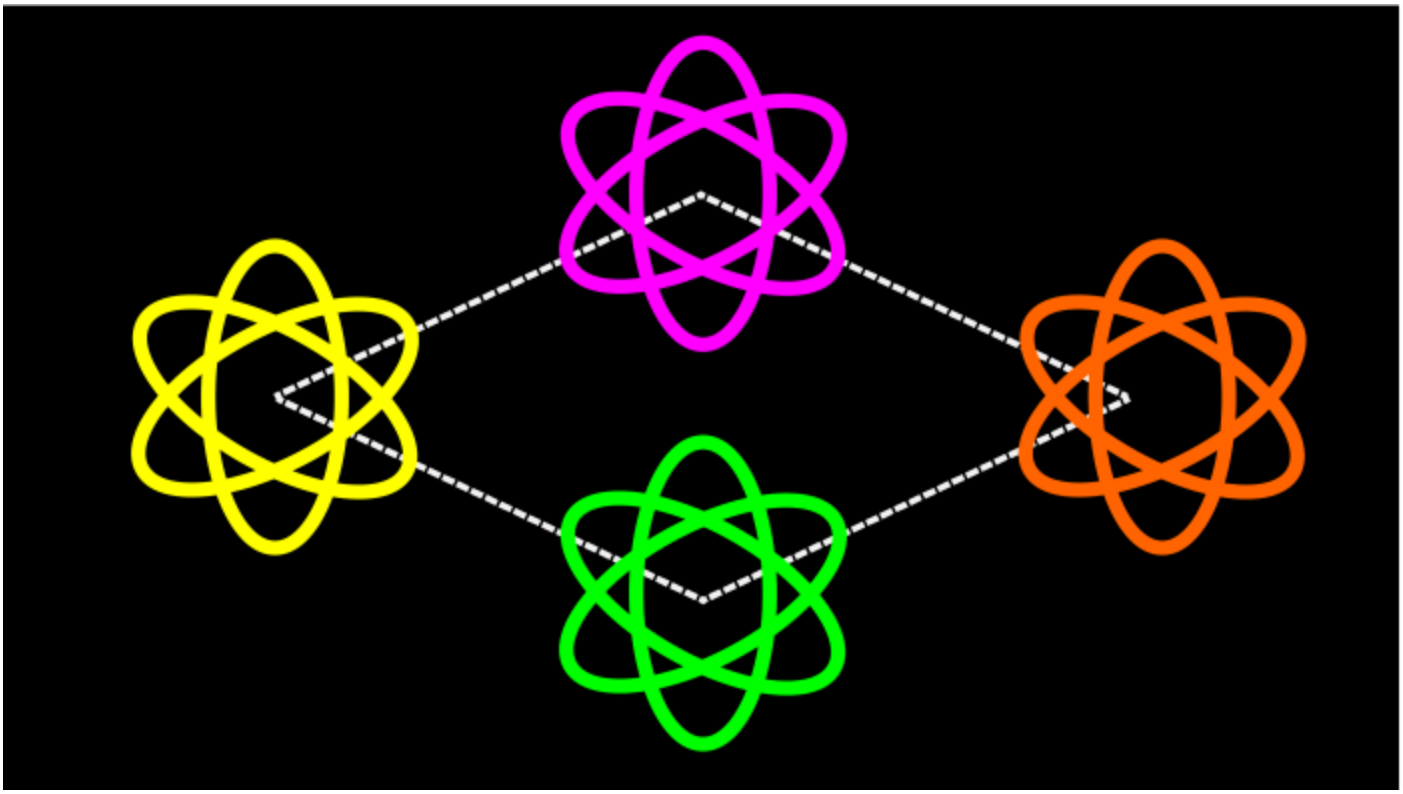


Figure 2.
The photon received by Alice interacts with a qubit of hers that contains quantum data. She measures the state of the entangled photon and this qubit at the same time. This measurement changes the state of Bob's entangled photon.

BOB

Researchers in the US, China, and Europe are racing to create teleportation networks capable of distributing entangled photons. But getting them to scale will be a massive scientific and engineering challenge. The many hurdles include finding reliable ways of churning out lots of linked photons on demand, and maintaining their entanglement over very long distances—something that quantum repeaters would make easier.

Still, these challenges haven't stopped researchers from dreaming of a future quantum internet.



What is a quantum internet?

Just like the traditional internet, this would be a globe-spanning network of networks. The big difference is that the underlying communications networks would be quantum ones.

It isn't going to replace the internet as we know it today. Cat photos, music videos, and a great deal of non-sensitive business information will still move around in the form of classical bits. But a quantum internet will appeal to organizations that need to keep particularly valuable data secure. It could also be an ideal way to connect information flowing between quantum computers, which are increasingly being made available through the computing cloud.

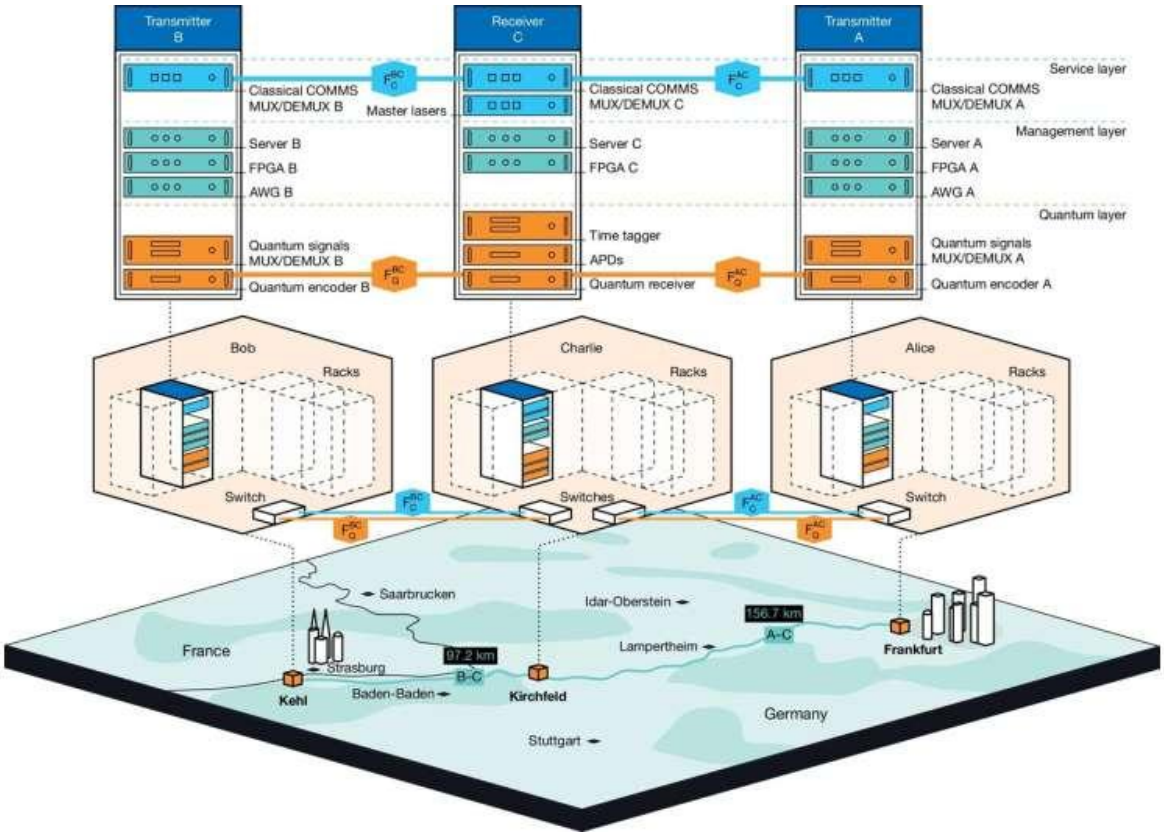
China is in the vanguard of the push toward a quantum internet. It launched a dedicated quantum communications satellite called Micius a few years ago, and in 2017 the satellite helped stage the world's first intercontinental, QKD-secured video conference, between Beijing and Vienna. A ground station already links the satellite to the Beijing-to-Shanghai terrestrial network. China

plans to launch more quantum satellites, and several cities in the country are laying plans for municipal QKD networks.

Some researchers have warned that even a fully quantum internet may ultimately become vulnerable to new attacks that are themselves quantum based. But faced with the hacking onslaught that plagues today's internet, businesses, governments, and the military are going to keep exploring the tantalizing prospect of a more secure quantum alternative.

APRIL 23, 2025

Quantum messages travel 254 km using existing infrastructure for the first time



by Nature Publishing Group

Deployed coherent quantum communications system. Credit: *Nature* (2025). DOI: 10.1038/s41586-025-08801-w
Quantum messages sent across a 254-km telecom network in Germany represent the first known report of coherent quantum communications using existing commercial telecommunication infrastructure.

The demonstration, reported in *Nature* this week, suggests that quantum communications can be achieved in real-world conditions.

Quantum networks have the potential to enable secure communications, such as a quantum internet; quantum key distribution is one example of a theoretically secure communication technique.

Exploiting the coherence of light waves (their potential to interact predictably) can extend the range of quantum communications, but scalability has been limited by the need for specialized equipment, such as cryogenic coolers.

An approach that enables the distribution of quantum information through optical fiber cables, without the need for cryogenic cooling, is described by Mirko Pittaluga and colleagues.

Their system uses a coherence-based twin-field quantum key distribution, which facilitates the distribution of secure information over long distances.

The quantum communications network was deployed over three telecommunication data centers in Germany (Frankfurt, Kehl and Kirchfeld), connected by 254 km of commercial optical fiber—a new record distance for real-world and practical quantum key distribution, according to the authors.

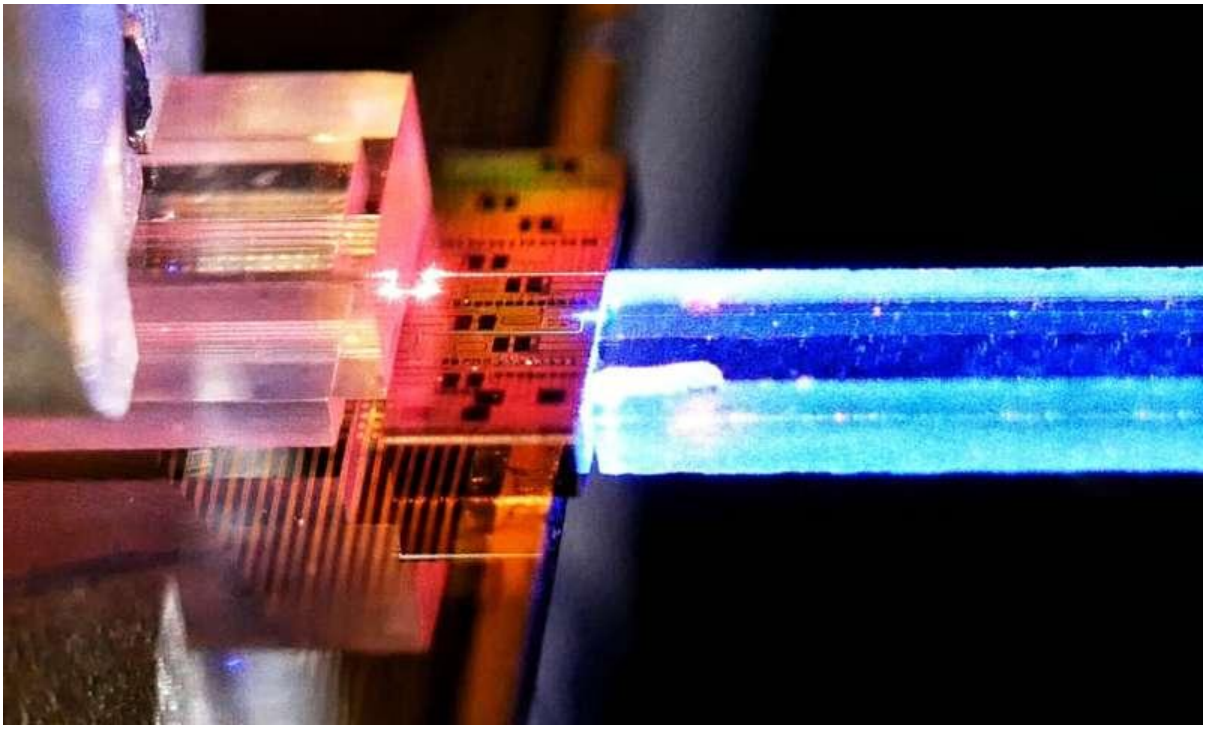
This demonstration indicates that advanced quantum communications protocols that exploit the coherence of light can be made to work over existing telecom infrastructure.

More information: Mirko Pittaluga et al, Long-distance coherent quantum communications in deployed telecom networks, *Nature* (2025). DOI: 10.1038/s41586-025-08801-w
Journal information: Nature
Provided by Nature Publishing Group

MAY 6, 2025

Single-photon technology powers 11-mile quantum communications network between two campuses

by Luke Auburn , University of Rochester



Network IT: A photonic chip coupled to a highly nonlinear crystal and a fiber array unit. The crystal produces entangled visible-telecom photon pairs, which are processed on silicon nitride and silicon photonic integrated circuits enabling a compact and versatile platform to link visibly accessed quantum nodes over existing telecommunications infrastructure. Credit: RIT

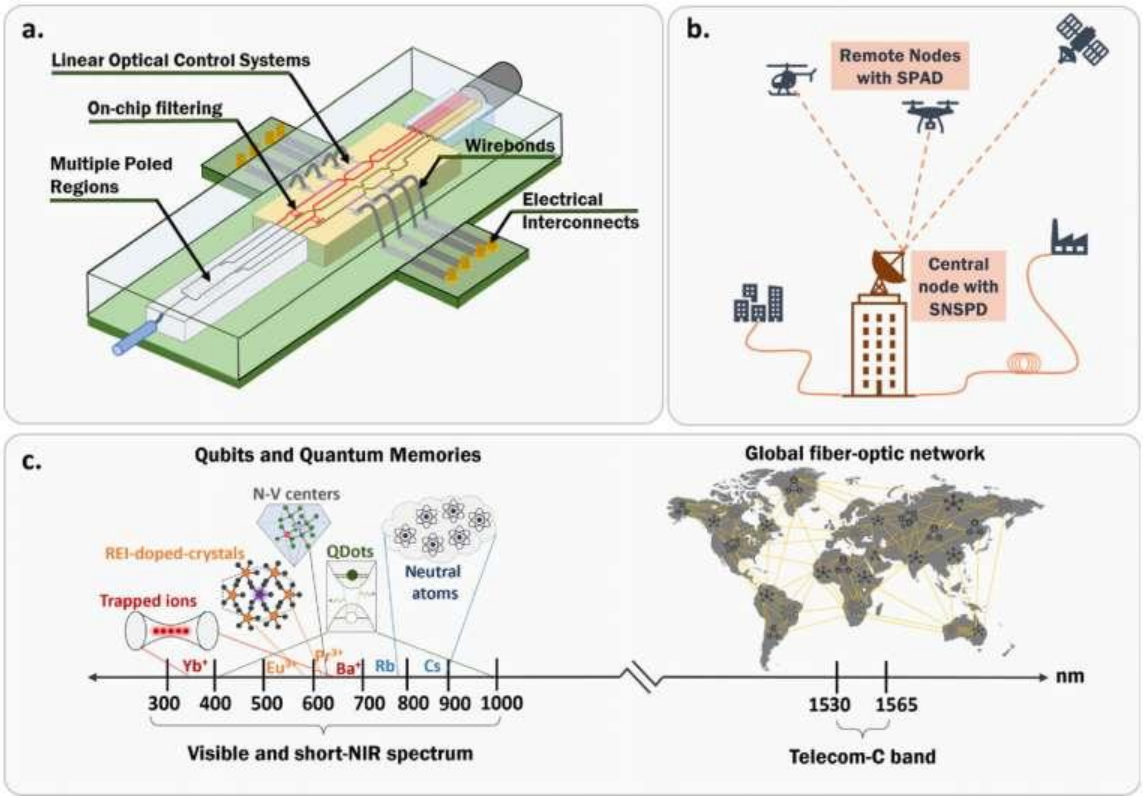
Researchers at the University of Rochester and Rochester Institute of Technology recently connected their campuses with an experimental quantum communications network using two optical fibers. In a new paper published in *Optica Quantum*, scientists describe the Rochester Quantum Network (RoQNET), which uses single photons to transmit information about 11 miles along fiber-optic lines at room temperature using optical wavelengths.

Quantum communications networks have the potential to massively improve the security with which information is transmitted, making messages impossible to clone or intercept without detection. Quantum communication works with quantum bits, or qubits, that can be physically created using atoms, superconductors, and even in defects in materials like

diamond. However, photons—individual particles of light—are the best type of qubit for long distance quantum communications.

Photons are appealing for quantum communication in part because they could theoretically be transmitted over existing fiber-optic telecommunications lines that already crisscross the globe. In the future, many types of qubits will likely be utilized because qubit sources, like quantum dots or trapped ions, each have their own advantages for specific applications in quantum computing or different types of quantum sensing.

However, photons are the most compatible with existing communications lines. The new paper is focused on making quantum communication between different types of qubits in a network a reality.



Scope. (a) A representative, fully packaged version of this platform incorporating multiple poled waveguides and on-chip filters for a plug-and-play source of visible–telecom entangled photon pairs. (b) Using a visible–telecom photon pair source enables the generation of telecom single photons heralded by the visible photons. Visible wavelengths can be efficiently detected using compact single-photon avalanche diodes, while telecom wavelengths are ideal for low-loss transmission across long distances in optical fibers. Our visible–telecom pair source would allow chip-scale, field-deployable quantum nodes to securely communicate with a central server using single photons at telecom wavelengths over existing optical fibers. (c) Our visible–telecom photon pair source also paves the way for an heterogeneous quantum network by bridging the gap between various visibly accessed quantum nodes and existing telecommunication infrastructure. Credit: *Optica Quantum* (2025). DOI: 10.1364/OPTICAQ.546774

"This is an exciting step creating quantum networks that would protect communications and empower new approaches to distributed computing and imaging," says Nickolas Vamivakas, the Marie C. Wilson and Joseph C. Wilson Professor of Optical Physics, who led the University of Rochester's efforts.

"While other groups have developed experimental quantum networks, RoQNET is unique in its use of integrated quantum photonic chips for quantum light generation and solid-state based quantum memory nodes."

The teams at the University of Rochester and RIT combined their expertise in optics, quantum information, and photonics to develop technology with photonic-integrated circuits that could facilitate the quantum network. Currently, efforts to leverage fiber-optic lines for quantum communication require bulky and expensive superconducting-nanowire-single-photon-detectors (SNSPDs), but they hope to eliminate this barrier.

"Photons move at the speed of light and their wide range of wavelengths enable communication with different types of qubits," says Stefan Preble, professor in the Kate Gleason College of Engineering at RIT. "Our focus is on distributed quantum entanglement, and RoQNET is a test bed for doing that."

Ultimately, the researchers want to connect RoQNET to other research facilities across New York State at Brookhaven National Lab, Stony Brook University, Air Force Research Laboratory, and New York University.

More information: Vijay S. S. Sundaram et al, Heralded telecom single photons from a visible–telecom pair source on a hybrid PPKTP–PIC platform, *Optica Quantum* (2025). DOI: 10.1364/OPTICAQ.546774
Provided by University of Rochester

Groundbreaking amplifier could lead to 'super lasers' that make the internet 10 times faster

News By Peter Ray Allison last updated June 2, 2025

Scientists have designed an amplifier that can transmit 10 times more information per second than current fiber-optic systems can, which could be helpful for medical treatment and diagnosis.

(Image credit: Baac3nes via Getty Images)

Scientists have developed a new type of laser amplifier that can transmit information 10 times faster than current technology.
Laser amplifiers boost the intensity of light beams. This particular amplifier achieves a tenfold increase in transmission speed by expanding the bandwidth, or wavelengths of light, at which the lasers can transmit information.

The amount of information we generate and transmit is growing every day. Due to the proliferation of streaming services, smart devices and generative AI, Nokia Bell Labs predicted in their Global Network Traffic Report that the amount of data traffic will double by 2030.
Current optical-based telecommunication systems transmit information by sending pulses of laser light through fiber-optic cables, which are thin strands of glass. The capacity — the amount of information that can be transmitted — is determined by the amplifier's bandwidth (the wavelengths of light that it can amplify). As data traffic increases, bandwidth therefore becomes crucial.

Most lasers used for modern telecommunications, such as internet communications, require an amplifier. These work by a process called stimulated emission, which uses an incoming photon to stimulate the release of another photon with the same energy and direction.

Scientists have now designed a new type of laser technology that can transmit information using a technology called high-efficiency optical amplification. The researchers published their findings April 9 in the journal Nature.
"The amplifiers currently used in optical communication systems have a bandwidth of approximately 30 nanometers," lead author Peter Andrekson, a professor of photonics at Chalmers University of Technology in Sweden, said in a statement. "Our amplifier, however, boasts a bandwidth of 300 nanometers, enabling it to transmit ten times more data per second than those of existing systems."
The new amplifier is made of silicon nitride, a hardened ceramic material that is resistant to high temperatures. The amplifier uses spiral-shaped waveguides to efficiently direct the laser pulses to remove anomalies from the signal. The technology has also been miniaturized so that multiple amplifiers can fit onto a small chip.

The researchers chose spiral waveguides over other waveguide types because they enable longer optical paths to be created within a small area. This enhances useful effects such as four-wave mixing, which occurs when two or more optical frequencies are combined together to amplify the output with minimal noise (external interference that can disrupt the quality of the signal).

Because the speed of light is constant, the laser light itself does not travel any faster than that from conventional lasers. However, the larger bandwidth enables the new amplifier to transmit 10 times more data than conventional lasers can.

The amplifier currently functions in a wavelength range of light 1,400 to 1,700 nanometers, which is within the short-wave infrared range. The next stage in the research will be to see how it operates over other wavelengths, such as those for visible light (400 to 700 nanometers) and a broader range of infrared light (2,000 to 4,000 nanometers).

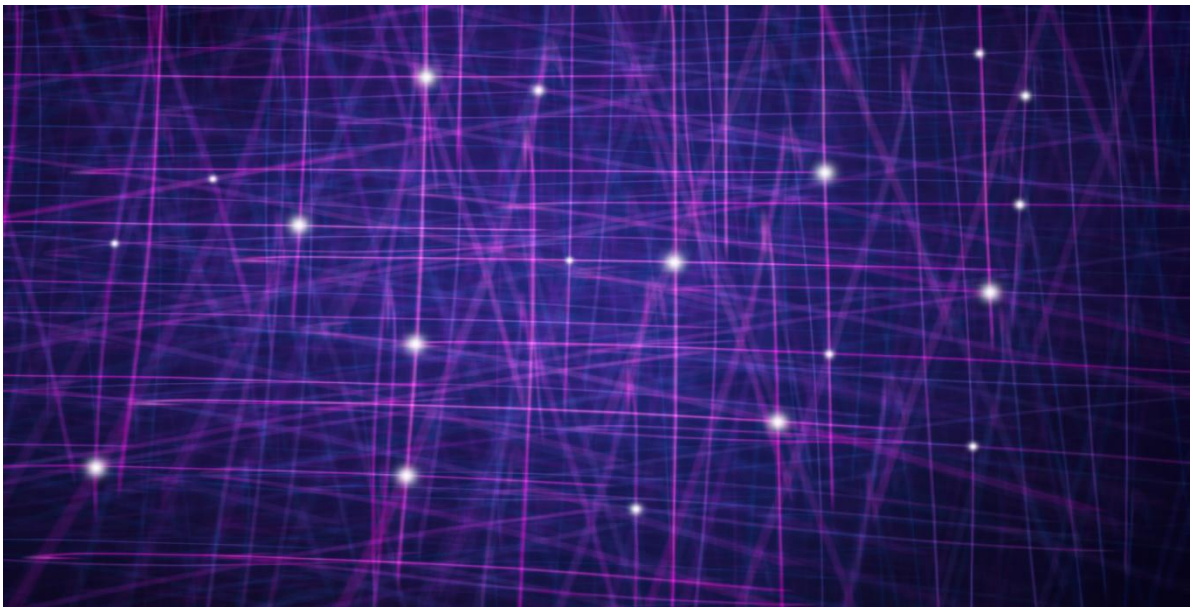
The new amplifier has multiple potential applications, including medical imaging, holography, spectroscopy and microscopy, according to the statement. The miniaturization of the technology could also make lasers for light-based applications smaller and more affordable.

"Minor adjustments to the design would enable the amplification of visible and infrared light as well," Andrekson said. "This means the amplifier could be utilised in laser systems for medical diagnostics, analysis, and treatment. A large bandwidth allows for more precise analyses and imaging of tissues and organs, facilitating earlier detection of diseases."

'Quantum memory breakthrough' may lead to a quantum internet

News By Peter Ray Allison published February 26, 2024

A new technique in quantum storage that operates at room temperature could pave the way for a quantum internet.



As well as being faster, quantum communications are inherently secure — while classical communications can be intercepted or manipulated. (Image credit: PM Images via Getty Images)

We're now one step closer to a "quantum internet" — an interconnected web of quantum computers — after scientists built a network of "quantum memories" at room temperature for the first time.

In their experiments, the scientists stored and retrieved two photonic qubits — qubits made from photons (or light particles) — at the quantum level, according to their paper published on Jan. 15 in the Nature journal, Quantum Information.
The breakthrough is significant because quantum memory is a foundational technology that will be a precursor to a quantum internet – the next generation of the World Wide Web.

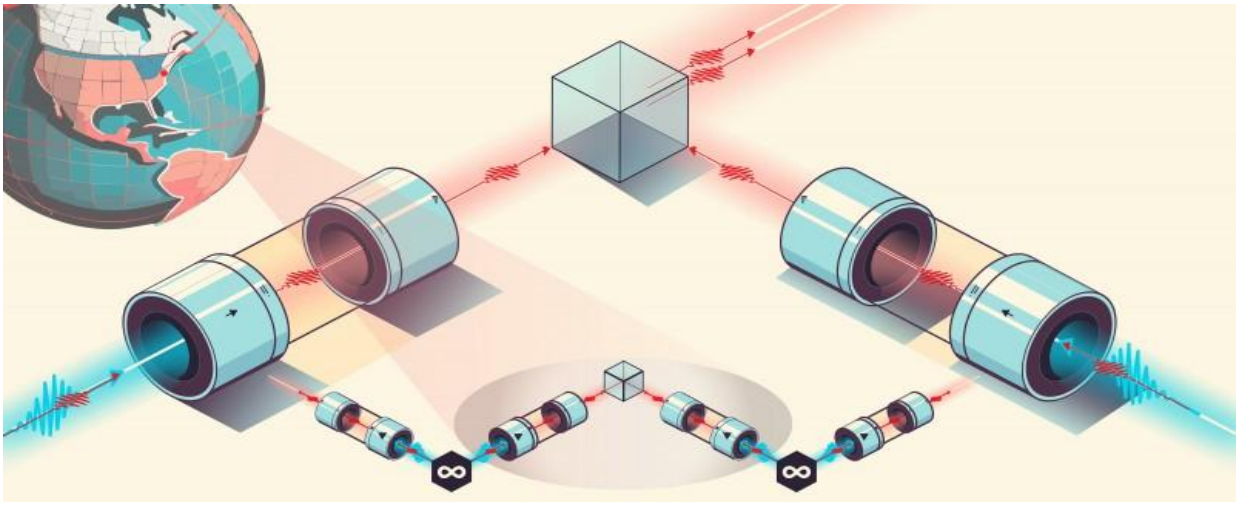
Quantum memory is the quantum version of binary computing memory. While data in classical computing is encoded in binary states of 1 or 0, quantum memory stores data as a quantum bit, or qubit, which can also be a superposition of 1 and 0. If observed, the superposition collapses and the qubit is as useful as a conventional bit.

Quantum computers with millions of qubits are expected to be vastly more powerful than today's fastest supercomputers — because entangled qubits (intrinsically linked over space and time) can make many more calculations simultaneously.

As the name implies, the quantum internet is an internet infrastructure that relies on the laws of quantum mechanics to transmit data between quantum computers. But we need quantum memory for a quantum network to function. Because qubits adopt a superposition of 1 and 0, rather than either binary state as in classical computing, they can store and transmit more information with far greater density than conventional networks. "To get these fleets of quantum memories to work together at a quantum level, and in a room temperature state, is something that is essential for any quantum internet on any scale. To our knowledge, this feat has not been demonstrated before, and we expect to build on this research," said lead author Eden Figueroa, professor of physics and astronomy at Stony Brook University, in a statement.

Building a network for quantum computing

Quantum networks built in recent years have needed to be cooled to absolute zero to operate, which limits their usefulness. But scientists from Stony Brook University developed a method to store two separate photons and – most importantly – successfully retrieve their quantum signature. They achieved this at room temperature by storing photons in a rubidium gas.
This makes it more viable than previous experiments in designing and deploying a quantum internet in the future. However, they could only store the photons in this experiment for a fraction of a second, while storing qubits at cryogenic temperatures normally means they can last for more than an hour.



Quantum repeaters require two sources of entangled photon pairs separated by a distance — where one photon is sent towards a quantum memory store, and the other photon is sent in the opposite direction. (Image credit: Chase Wallace, Stony Brook University)

"The actual selling point of this was that they were able to take two independently stored photons, retrieve them at the same time, and interfere them," Daniel Oi, a professor in

quantum physics at the University of Strathclyde, told Live Science. “You get what’s called a HOM dip, or a Hong-Ou-Mandel dip, which is a characteristic quantum signature indicating that these two photons were identical.”
As well as being faster, quantum communications are inherently secure — while classical communications can be intercepted or manipulated. This is because any attempts to intercept and read information transmitted across the quantum network equates to observation — which would collapse the superposition of the qubits moving through the circuit.

This is an active field of research and a race is underway to develop the technologies that will help us build a quantum internet. In 2022, researchers in Switzerland stored a single photon using a similar method. That same year, China transmitted signals using quantum entanglement between two memory devices located 12.5 kilometers apart.
The next stage is to develop a method for detecting when a quantum signal is ready to be retrieved, without destroying the properties of the signal through direct observation. Achieving this would pave the way for quantum repeaters, which are devices that can extend the range of a quantum signal. This would be a key precursor to a large-scale quantum internet.

“One of the holy grails of quantum memories is ‘How do you detect that you’ve actually stored a photon, without destroying the quantum properties of that photon, and do it in a way that is efficient and reliable?’,” said Oi.

Quantum networking: A critical bridge to utility-scale quantum computing

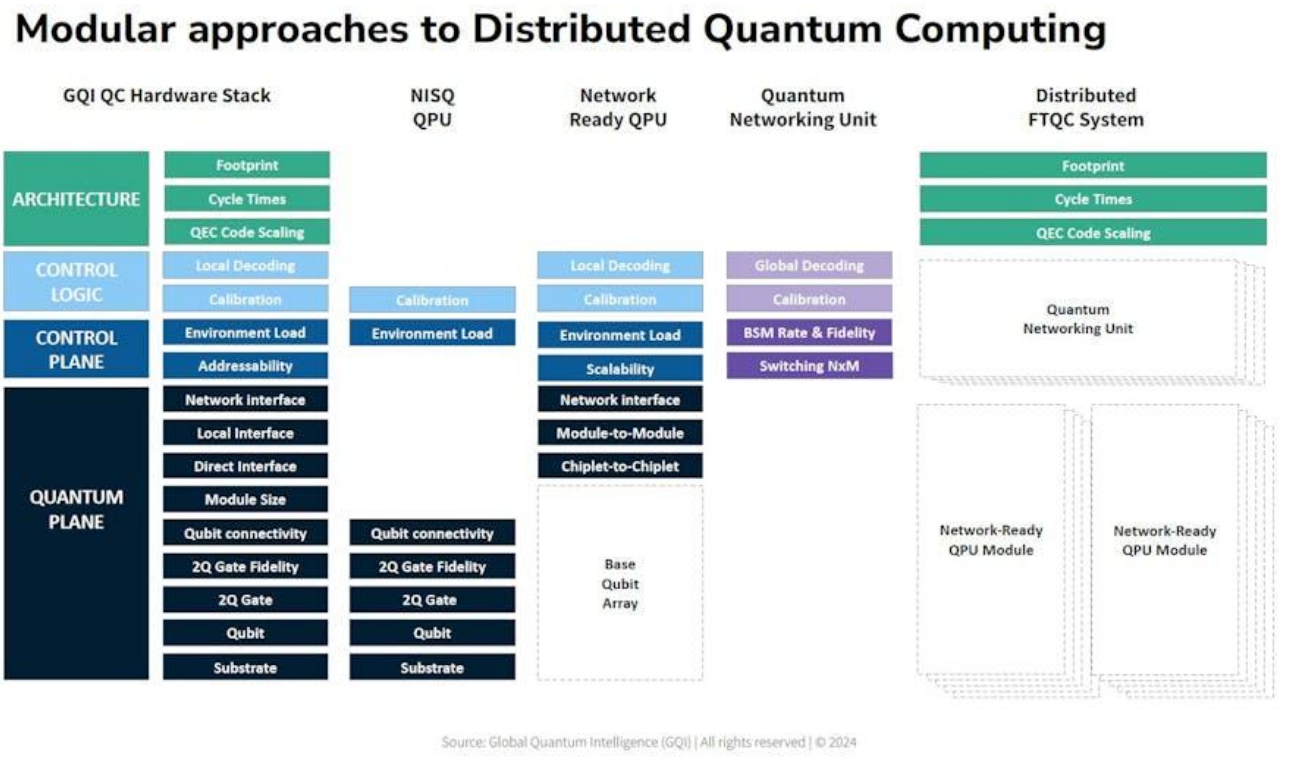
For the photonics community, quantum networking is an opportunity to provide the critical infrastructure that transforms quantum computing into a world-changing technology. July 2, 2025

ID 330304019 © Oleksandra Tsvid | Dreamstime.com

The quantum computing industry faces a fundamental scaling bottleneck that threatens to strand us in the era of noisy intermediate-scale quantum (NISQ) devices. While today's leading systems boast hundreds of qubits, the transformative applications we seek—drug discovery, materials science, and cryptanalysis—demand fault-tolerant machines with millions of physical qubits. The harsh reality? No single quantum processing unit (QPU) can feasibly house that many qubits.

Consider the physical constraints across today's quantum platforms. Superconducting circuits, limited by the cooling power of dilution refrigerators at 20 millikelvin (mK), cap out around 3,000 qubits per module (see Fig. 1). Trapped ion systems face stability limits in linear chains (100 qubits) or untested scaling in quantum charge-coupled device (QCCD) architectures. Even neutral atom arrays, despite their impressive 10,000-qubit potential, bump against optical aperture and laser power

ceilings. Silicon spin qubits promise “millions” on paper, but thermal management at 1 K remains unproven.



Credit: GQI

FIGURE 1. Physical constraints limit viable module sizes across quantum computing platforms. Cooling power, optical apertures, and control complexity create hard ceilings that networking must overcome.

The solution mirrors classical computing’s evolution: Modular, networked architectures (see Fig. 2). Just as data centers link thousands of processors, quantum computing must embrace distributed architectures where multiple quantum processing unit (QPU) modules collaborate through quantum networking. This isn’t merely about connecting boxes—it requires preserving the delicate quantum entanglement that gives these machines their power. This is where photonics emerges as a natural bridge and offers low-loss transmission of quantum states through optical fibers and the ability to generate entanglement between distant qubits via photon-mediated interactions.

Credit: GQI

FIGURE 2. Distributed quantum computing architectures enable scaling beyond single-module limits through quantum networking units that preserve entanglement while connecting multiple QPU modules.

Viable module scale varies by qubit platform

GQI

GQI target module size assessments (first generation architectures)

Manhattan Project dynamics?

Platform	Type	Dim. um	Key Factor	Unit cell mm2	Die mm2	Unit cell per chiplet	Qubits per module	Notes
SC Circuits	Transmon	600	Circuitry	0.36	800	2,222	3,000	Ass. 100uW @ 20mK (super firdge)
Trapped Ion	Linear Trap	5	Ion spacing	n/a	n/a	100	100	Limited by ion crystal stability
	QCCD	100	Ion height	1	800	800	un-tested	
		40	Ion height	0.16	800	5,000	un-tested	Low ion height may impact fidelity
Neutral Atom	2D lattice	6	Atom spacing	3.60E-05	n/a	10,000	10,000	Limited by optical aperture & laser power
Photonics	Dual rail	150	SiN bend	2.25E-02	800	200	200	Ass. NxN interferometer
Silicon Spin	Exchange interaction	12	Control electronics	1.44E-04	800	5,000,000	1,000,000	Ass. 100mW @ 1K
Colour Center	Barrett-Kok	250	Fiber array pitch	6.25E-02	800	13,000	2,000	Yield
Topological	MZM	10	Nanowire array	1.00E-04	800	8,000,000	100,000 + *	Cooling power @ 50-100mK?

** Microsoft marketing claims 1million*

From vision to venture capital: Modular won. Here's the proof.

Global Quantum Intelligence (GQI) identified this modular imperative more than three years ago and began advocating for distributed architectures while the industry still chased monolithic “Goliath” designs. Our May 2024 report “Scalable Quantum Hardware” mapped the technical requirements for quantum networking units (QNUs) that can bridge QPU modules while maintaining fault-tolerant operation.

The subsequent 12 months validated this vision spectacularly. The quantum networking sector has attracted significant funding and key developments emerged:

- **Xanadu Aurora** (January 2025): Achieved 12-qubit universal photonic quantum computer across 4 modular server racks interconnected via 13 kilometers of fiber, synthesizing an 86.4 billion mode cluster state.
- **PsiQuantum Omega** (February 2025): Unveiled chipset networking 35 photonic chips with 99.72% chip-to-chip quantum interconnect fidelity over distances up to 250 meters.
- **Nu Quantum QNU** (June 2025): Launched world’s first rack-mounted QNU with 99.7% entanglement fidelity and sub-microsecond circuit switching.
- **Welinq** (March 2025): Launched commercial quantum memory achieving world-record 90% storage-and-retrieval efficiency with 200-microsecond storage duration.

- **Sparrow Quantum** (April 2025): Secured €21.5M ($25.1M) Series A for deterministic single-photon sources, building on Danish quantum photonics leadership.
- **Lightsynq** (November 2024): Raised $18M for diamond-based optical quantum interconnects, subsequently acquired by IonQ in May 2025.
- **SilQ Connect** (May 2025): Launched from Sherbrooke, Canada with pre-seed funding for microwave-optical quantum interconnects enabling quantum local area networks.
- **Cisco's quantum chip** (May 2025): Room-temperature operation generates 200 million entangled photon pairs per second.

Even traditionally monolithic players now embrace modularity. IBM's 2025 roadmap features "l-type" meter-scale quantum links between dilution fridges. IonQ's acquisition spree—Oxford Ionics, Lightsynq, ID Quantique—transforms it from a compute-only vendor into a full-stack quantum networking company. The Quantum Data Center Alliance, led by Nu Quantum, brings together Cisco, QphoX, Oxford Quantum Circuits, and others to standardize interfaces for building-scale quantum networks.

Credit: GQI

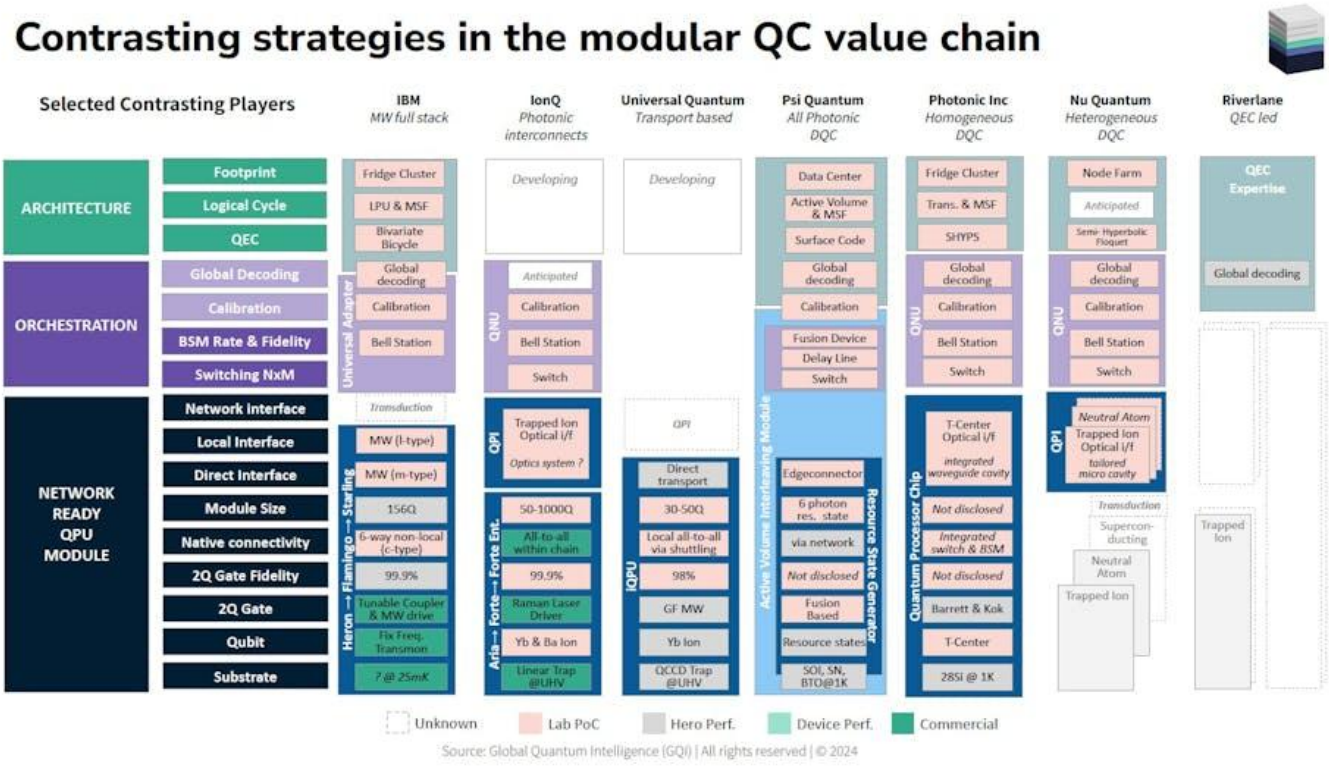


FIGURE 3. Contrasting strategies in the modular quantum computing value chain reveal how photonic technologies enable different paths to scalability.

Photonic value chain: Who owns the quantum highway?

The race to build quantum networks has crystallized distinct strategies across the photonic value chain (see Fig. 3). Each approach reveals different bets on how light will enable million-qubit machines:

Homogeneous integration. Photonic Inc. pursues silicon T-centers (carbon-based color center) that natively combine spin qubits with optical interfaces within the same material platform. Their integrated waveguide cavities promise efficient qubit-photon interfaces without heterogeneous assembly.

Heterogeneous enablement. Nu Quantum develops high-performance photonic cavities compatible with multiple qubit platforms—trapped ions, neutral atoms, and color centers. Their QNU's modular architecture allows optical modules to be swapped to support different qubit types, positioning them as the essential middleware provider.

All-photonic computing. PsiQuantum and Xanadu need no qubit-photon interface; photons serve as both qubits and interconnects. PsiQuantum's Active Volume architecture and Xanadu's squeezed-light approach use optical switching and delay lines to create data center-scale quantum computers from networked photonic chips.

Critical supporting technologies span the photonic spectrum:

- **Single-photon sources** (Sparrow Quantum, Qunnect): Deterministic generation for high-fidelity entanglement—Sparrow's on-chip sources set industry benchmarks.
- **Quantum memories** (Welinq, MemQ): Store and synchronize entanglement—Welinq's room-temperature operation eliminates cryogenic requirements.
- **Transducers** (QphoX, SilQ Connect): Convert between microwave and optical domains.
- **Single-photon detectors** (ID Quantique, Single Quantum, Quantum Opus): Enable high-efficiency Bell state measurements.

The ecosystem extends beyond these specialized components, with many other photonic players advancing the field—Aegiq, ORCA Computing, Quandela, QuiX Quantum, and Quantum Source—each contributing unique approaches to photonic quantum computing and networking.

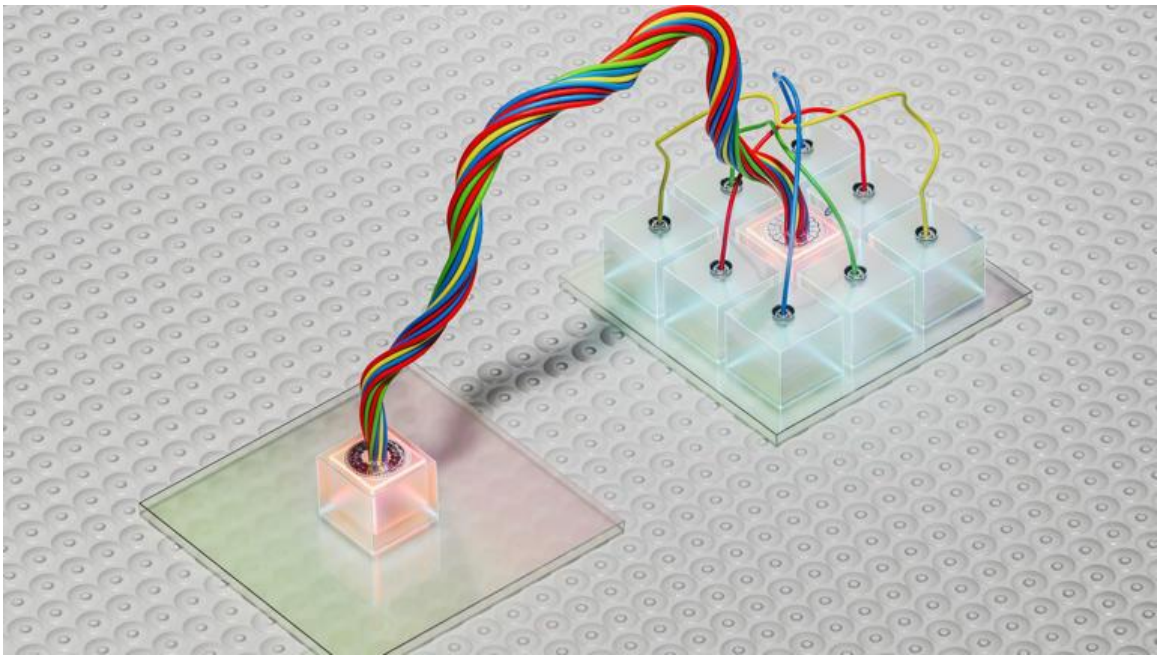
The message is clear: Quantum networking isn't a future consideration—it's the present battlefield where quantum computing's leaders will be determined. For the photonics community, this represents a generational opportunity to provide the critical infrastructure that transforms quantum computing from laboratory curiosity to world-changing technology. The path to a million qubits can run through optical

fiber, and those who master quantum networking will define the next era of computation.

FURTHER READING

GQI Outlook Report; Scalable Quantum Hardware:
www.global-qi.com/product-page/outlook-report-scalable-quantum-hardware

World's first quantum teleportation sends telecom qubit into solid-state memory device



World's first quantum teleportation sends telecom qubit into solid-state memory device

Quantum teleportation, once the stuff of science fiction, is rapidly becoming a central pillar in the race to build the next version of the internet.

Instead of transmitting particles or signals through wires or airwaves, this process transfers the quantum state of a particle from one place to another, instantly and without physically moving the particle itself.

It works by leveraging quantum entanglement, a phenomenon where two particles become so deeply connected that the state of one instantly affects the other, no matter how far apart they are.

In a significant step toward building a scalable quantum internet, researchers at Nanjing University have demonstrated quantum teleportation of a telecom-wavelength photonic qubit to a solid-state quantum memory.

This marks the first time such a feat has been achieved using telecom-compatible equipment, offering a path to integrate quantum networks with today's communication infrastructure.

Experiment uses fiber-friendly tech

Led by senior author Xiao-Song Ma, the team successfully transferred quantum information from a photon to a solid-state memory based on erbium ion ensembles.

Unlike earlier teleportation efforts that relied on frequency conversion, this experiment operated entirely in the telecom band, the same range used in conventional fiber-optic communication.

"Quantum teleportation is always a fascinating protocol in quantum communication for its ability to transfer quantum states without ever revealing," Ma told *Phys.org*.

The goal was to integrate a solid-state memory with the teleportation process, enabling temporary storage of quantum states for long-distance transmission.

In quantum networks, such memory units are vital for distributing entanglement and ensuring stable communication across large distances.

"To extend the state transmission distance further, the incorporation of quantum memory into a quantum teleportation system is of critical importance," Ma said.

Quantum networks function with the help of repeaters, which divide long links into smaller sections.

By placing quantum memories at these endpoints, information can be stored until entanglement is established across all links, forming the backbone of a future quantum internet.

Five-part system delivers results

Ma's team deployed five interconnected systems to pull off the experiment.

These included input state preparation, an entangled photon source (EPR-source) created on an integrated photonic chip, a Bell-state measurement module, and the erbium-based quantum memory.

They also employed a frequency distribution and fine-tuning setup using a Fabry-Pérot cavity and the Pound-Drever-Hall (PDH) technique for precise signal alignment.

"Our study demonstrated the quantum teleportation from telecom photons to a solid-state quantum memory based on erbium ions for the first time," Ma said. "Our entire system uses components compatible with existing fiber networks perfectly."

That compatibility is a major milestone.

Most prior systems required converting signals to different frequencies, limiting real-world deployment.

By staying in the telecom band, this setup works seamlessly with today's infrastructure.

"This telecom-compatible platform for generating, storing and processing quantum states of light establishes a highly promising approach to large-scale quantum networks," Ma added.

The team now plans to refine the solid-state memory system.

Their next focus includes extending storage duration and boosting the efficiency of data retention, both critical for practical quantum networking.

With this breakthrough, the road to a functional quantum internet just became clearer and more fiber-ready.

The study is published in the journal *Physical Review*

JULY 21, 2025

Quantum internet moves closer as researchers teleport light-based information

by Ingrid Fadelli, Phys.org edited by Gaby Clark, reviewed by Andrew Zinin

Quantum teleportation is a fascinating process that involves transferring a particle's quantum state to another distant location, without moving or detecting the particle itself. This process could be central to the realization of a so-called "quantum internet," a version of the internet that enables the safe and instant transmission of quantum information between devices within the same network.

Quantum teleportation is far from a recent idea, as it was experimentally realized several times in the past. Nonetheless, most previous demonstrations utilized frequency conversion rather than natively operating in the telecom band.

Researchers at Nanjing University recently demonstrated the teleportation of a telecom-wavelength photonic qubit (i.e., a quantum bit encoded in light at the same wavelengths supporting current communications) to a telecom quantum memory. Their paper, published in *Physical Review Letters*, could open new possibilities for the realization of scalable quantum networks and thus potentially a quantum internet.

"Quantum teleportation is always a fascinating protocol in quantum communication for its ability to transfer quantum states without ever revealing," Xiao-Song Ma, senior author of the paper, told Phys.org. "To extend the state transmission distance further, the incorporation of quantum memory into a quantum teleportation system is of critical importance."

The main objective of the recent study by Ma and his colleagues was to successfully integrate a telecom solid-state quantum memory into a quantum teleportation system, which would enable the storage of transmitted quantum information. The main role of this memory would be to spread and store entangled particles across a quantum network (i.e., entanglement distribution).

Quantum networks rely on quantum repeaters, devices that can break the distances across which information is transmitted into shorter and more manageable sections, known as elementary links. When placed at the end of these sections, quantum memories could store

quantum information for the time necessary for entanglement to be established across entire segments of networks, which could in turn enable its transmission across longer distances.

"We employed five systems to accomplish the experiment," explained Ma. "These include an Input state preparation; an EPR-source to generate entangled photon pairs from an integrated photonic chip, a Bell-state measurement and a quantum memory based on erbium ion ensembles. We also employed a frequency distribution and fine-tuning module based on an F-P cavity and PDH technique."

This recent work by Ma and his colleagues shows that quantum information could be transferred across a network using devices and optical wavelengths that are compatible with those currently employed in communications. The team's demonstration of quantum teleportation could inform the advancement of quantum networks, potentially contributing to the future realization of a reliable quantum internet.

"Our study demonstrated the quantum teleportation from telecom photons to a solid-state quantum memory based on erbium ions for the first time," added Ma. "Our entire system uses components compatible with existing fiber networks perfectly. This telecom-compatible platform for generating, storing and processing quantum states of light establishes a highly promising approach to large-scale quantum networks."

As part of their next studies, the researchers plan to focus on improving the performance of the erbium ion-based solid-state memory employed in their experiments. More specifically, they would like to extend its storage times and improve the efficiency with which it stores quantum information.

Written for you by our author Ingrid Fadelli, edited by Gaby Clark, and fact-checked and reviewed by Andrew Zinin—this article is the result of careful human work. We rely on readers like you to keep independent science journalism alive. If this reporting matters to you, please consider a donation (especially monthly). You'll get an **ad-free** account as a thank-you.

More information: Yu-Yang An et al, Quantum Teleportation from Telecom Photons to Erbium-Ion Ensembles, *Physical Review Letters* (2025). DOI: 10.1103/3wh8-2gh1.
Journal information: Physical Review Letters

Interplanetary Internet: Sending Data Across the Solar System

The future LunaNet will bring terrestrial Internet capabilities

to astronauts, rovers, and orbiters.
Media Credit: NASA/Reese Patillo

July 23, 2025 • By Amelia Williamson Smith, Managing Editor

Imagine—your spacecraft lands at a future colony on Mars, and you're eager to explore life on a new planet. You see the dusty red terrain stretching to the horizon. Olympus Mons, the tallest volcano in the solar system, rises in the distance. You want to share photos with your family and

friends. But then you realize: there's no Internet. You can't communicate with others like you're used to.

You arrive at your new home and need to look up some information and send an email to your coworker, so you pull out your laptop. Suddenly, it hits you. You can't do that either. Frustrated, you decide to listen to some music, but then it dawns on you. There's no online music library on Mars. You can't watch your favorite TV shows and movies either.

You feel totally cut off and lost. Without the Internet, life as you know it is totally different.

As we look to a future where missions to other planets will not only be possible but commonplace, a key question looms: How will we communicate and transmit data? For nearly three decades, someone has been working on the solution—Vint Cerf, one of the two "fathers of the Internet" who co-developed the protocols that allow networks to connect.

It was the spring of 1998, and Cerf was excited by the success of the **NASA** National Aeronautics and Space Administration Mars Pathfinder mission and Sojourner, the first robotic rover to explore the Martian surface. As he envisioned a future where humans would one day set foot on the red planet, his mind shifted to an important question. "What should we be doing now that we're going to need 25 years from now for space communications?"

Dressed in his signature three-piece suit in his office at Google headquarters, where he now serves as the

company’s vice president and chief Internet evangelist, Cerf recalled a conversation he had with scientists at NASA’s Jet Propulsion Laboratory back in 1998. When he posed his question to the group, the answer became clear. “We needed to design an interplanetary backbone network to support human and robotic space exploration.”

Such a network would connect people across the solar system. But there are challenges to creating an interplanetary Internet—the distances data must travel are much longer, and there’s not always a connection as planets and satellites move and block the signal. To address these issues, Cerf co-led the development of Delay and Disruption Tolerant Networking (DTN), in which the network stores “bundles” of data at intermediate nodes until a reliable path to the next node or the final destination becomes available.

Alberto Montilla presented preliminary findings from Spatiam's **ISS** International Space Station technology demonstration at the 2024 Space-Terrestrial Internetworking Workshop in Mountain View, California.

Now, we are on the verge of the future Cerf envisioned. With plans for commercial space stations, sending astronauts back to the Moon, and human missions to Mars, the time has come to make interplanetary Internet a reality—and Spatiam Corporation is up for the challenge. The startup built a commercial platform for space communications based on DTN. However, to advance the technology, Spatiam needed to test it in the environment where it will operate: space. And to do that, the company

turned to the International Space Station (ISS) National Laboratory.
“The most important thing for us as a company is being able to gain the operational experience to manage networks in space, and having access to that through the ISS National Lab was a fantastic opportunity,” said Spatiam CEO and co-founder Alberto Montilla. “The ISS was the ideal place to demonstrate our DTN platform for interplanetary networking because it provides a real-life operational scenario.”

Overcoming Connectivity Challenges in Space

The Internet connects billions of devices worldwide, putting global communication and data transfer at our fingertips 24/7. When data is sent through the Internet, it is broken into smaller units called packets. These packets travel through network devices like routers that determine the best path for each packet to take. Once the packets arrive at their destination, they are reassembled to recreate the original data.

When you think about the Internet on Earth, it has two key characteristics, Montilla explained. One is immediacy—given the relatively short distances data must travel between locations on Earth, the connection speed is incredibly fast. Delays are on the order of milliseconds, which is quicker than the blink of an eye. The other is ubiquity—anyone can connect to the network from anywhere in the world at any moment.

However, in space, things are radically different. Instead of immediacy and ubiquity, there is delay and disruption.

Vint Cerf is pictured here during an ARPANET demonstration in 1974.
Media Credit: Keith Uncapher, USC/ISI

“When you go to space, especially when you think about going to the Moon, signal delays—the time it takes for radio or light waves to move from one place to another—are in seconds, and when you go to Mars, it’s minutes,” Montilla explained.

Disruption is also a problem. When sending data from the Moon or Mars to a location on Earth, the two points do not always have a direct line of sight, leading to gaps in connectivity. Even on the ISS, communication is not continuous. Each day, there are several brief disruptions as the ISS orbits Earth and moves in and out of contact with ground stations and satellites.

“The TCP/IP protocols we created for the terrestrial Internet work well in a relatively low-latency, high-connectivity environment, but they’re not so attractive when you get to the deep space environment,” Cerf said. “So, we started working on new protocols, which we now call the Bundle Protocol Suite, for DTN.”

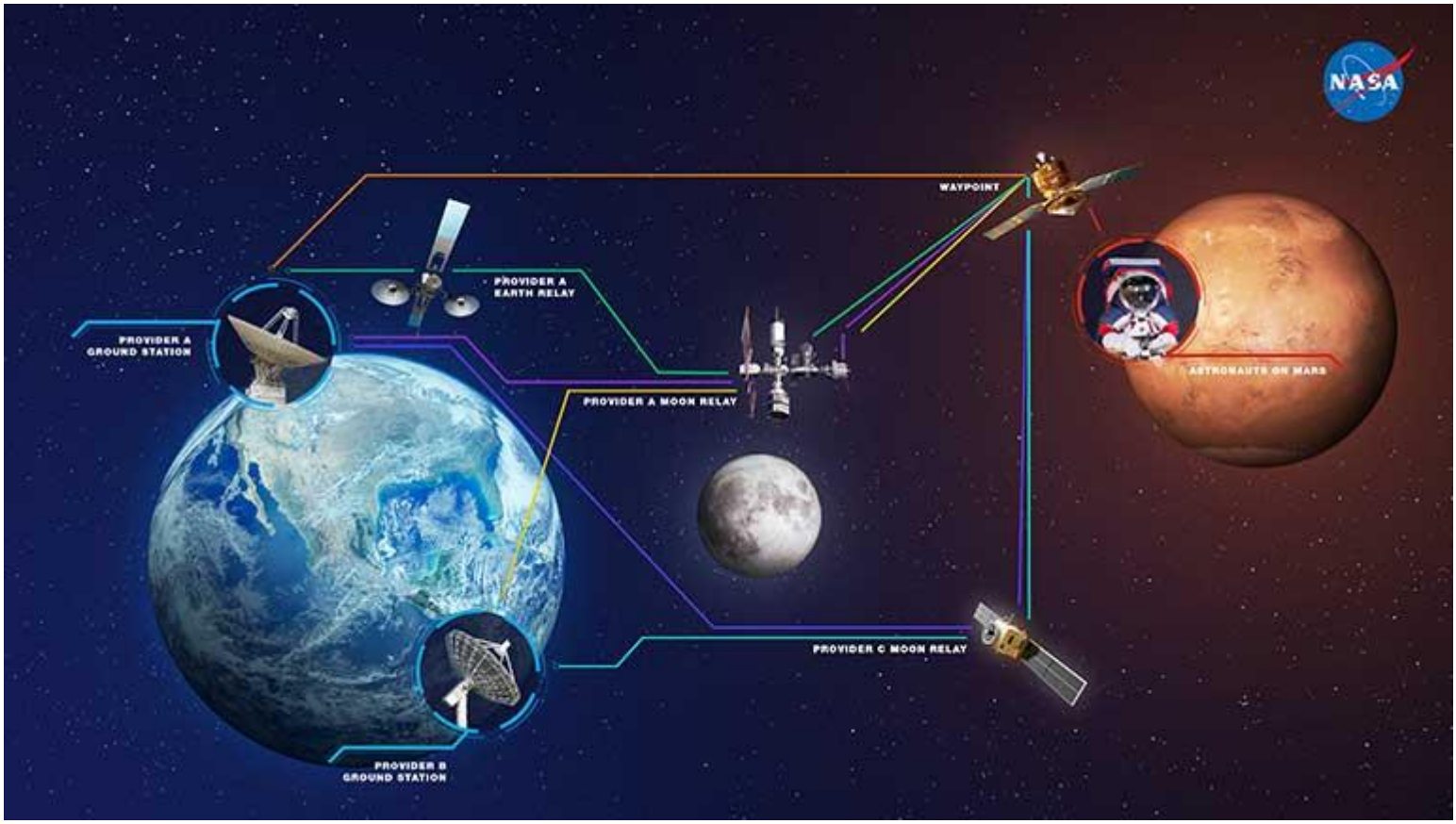
Enabling Reliable Communications

Currently, most data sent to and from space uses a direct link, which allows data to be sent from one entity to another when there is contact. The data moves from point A to point B—from the spacecraft to payload operations on the ground, for example. To transfer the data to a scientist at point C, a separate connection must be established.

It’s feasible to work around brief connectivity disruptions and manage contacts between one spacecraft, such as the ISS, and the operations team on the ground. However, managing contacts for a multitude of users sending data between Earth and commercial space stations or the Moon and Mars would be much more challenging, and a DTN platform will be vital.

“We’re moving from an entity that has been largely managed by a few space agencies to an entire ecosystem where there are going to be other government agencies along with a plethora of commercial companies of all types and sizes,” Montilla said.

By 2004, Cerf and his team had developed prototype software for DTN, and the first DTN operations on the ISS took place in 2009. Having reliable communications and navigation systems connecting space and Earth is crucial, said Philip Baldwin, assistant deputy associate administrator for the SCaN (Space Communications and Navigation) Program at NASA Headquarters in Washington.



Delay and Disruption Tolerant Networking (DTN) enables the use of multiple paths and providers to efficiently deliver data. (Click image for full size view)
Media Credit: NASA

“NASA uses DTN technology to safely store and forward data when a path opens,” Baldwin said. “Implementing these internetworking capabilities in space will decrease data loss, ensure data delivery, and provide mission teams with an ability to identify the location and timeline of data.”

From Nodes to Networks

Building on NASA’s extensive experience, Spatiam aims to develop the first commercial DTN platform for commercial

space stations and operations on the Moon and Mars. Spatiam's platform has three main elements: a DTN manager, DTN-managed instances (or nodes), and a DTN command line interface.
As its name suggests, the DTN manager directs the network, which is composed of several nodes. You can think of a network like a web, and each point where the web crosses is a node. You can transfer data from any point on the web to any other point by moving bundles of data from node to node until they reach the destination. The DTN manager configures the nodes to determine the best path for data to travel through the network. Through the DTN command line interface, users can send or request data without needing to know when contact occurs. Once the command is sent, the system holds the data and sends it during the next contact.

In addition to delivering core DTN capabilities, Spatiam's platform also provides advanced features that go beyond what's currently possible on the ISS. One such feature supports a service provider architecture that uses bundle-in-bundle encapsulation, where a bundle of data is carried inside another bundle. This allows the inner bundle to be transmitted more securely and reliably through the network. Another feature is the ability to stream audio and video, allowing future astronauts to transmit ultra-high-definition video from the Moon's surface to Earth, as is currently planned for NASA's Artemis missions. The platform also allows multiple administrators to access the network and control nodes.

A Steppingstone to Commercialization

To test its DTN platform, Spatiam worked with ISS National Lab **Commercial Service Provider** Implementation Partners that own and operate commercial facilities for the support of research on the ISS or are developing future facilities. Axiom Space, which provided the hardware for the investigation—an Amazon Snowcone edge computer on the space station. The Axiom team held weekly meetings with Spatiam to help navigate NASA requirements and daily meetings leading up to the ISS demonstration to resolve any issues.

“This is important because it’s very different from the NASA network, which is administered by NASA alone,” Montilla said. “We wanted to demonstrate that we can create networks that have many different administrators, similar to the way the Internet is on Earth.”

Throughout the project, Spatiam ran more than 95 unique tests and successfully validated the core capabilities of its DTN platform, the performance of its DTN manager, and the platform’s advanced features. The team tested the DTN manager’s ability to set up an initial network of four nodes (two on the ISS and two on Earth), add new nodes, and change node configuration.

Using the DTN platform, the team successfully transferred multiple types of data to and from the ISS, including telemetry data, text commands and responses, text files, and binary files. The platform also successfully streamed

audio and video. Bundle-in-bundle encapsulation—which had never been done in space before—was used during the entire 18-day demonstration.

With successful validation on the ISS, Spatiam raised the **technology readiness level**(Abbreviation: TRL) A measurement system used to assess the maturity level of a particular technology. There are nine technology readiness levels, and technology progresses from TRL 1 to TRL 9. (TRL) of its DTN platform to TRL 7, which is one step away from being flight-certified and ready for commercialization. Montilla stressed that access to the space station through the ISS National Lab was critical for advancing the company's platform.

By supporting the development of new technologies like DTN, the U.S. government lays the foundation for successful commercialization. Cerf explained, "The Internet spread, in part, because the government made early investments and then the private sector said, 'Oh, we can actually build and service and sell equipment and software to support the use of the Internet.' Many of the applications of the terrestrial Internet have come from the private sector, driven not by government investment but by the government-created potential for private-sector investment."

The Future of Networking in Space

Following Spatiam's successful validation, the company received recognition across the industry. "This was an amazing opportunity to demonstrate our platform, and it has opened so many doors for us," said Spatiam Business

Development Manager Veronica Acosta. “We are very proud of these accomplishments and look forward to what’s next in advancing the space economy.”

Spatiam’s goal is to enable the DTN portion of the future LunaNet network on the Moon. LunaNet will serve both NASA and lunar commercial service providers, paving the way for networking on future missions to Mars. Although not part of the startup’s original plan, after working with the ISS National Lab, Spatiam realized there are also significant opportunities for DTN in the future **LEO**(Abbreviation: LEO) The orbit around the Earth that extends up to an altitude of 2,000 km (1,200 miles) from Earth’s surface. The International Space Station’s orbit is in LEO, at an altitude of approximately 250 miles. economy.

“As commercial space stations start to fly and NASA begins using commercial facilities in LEO, we have identified use cases where our DTN platform is valuable,” Montilla said. “So, our plan is to expand our platform to support not only missions to the Moon and Mars but also in LEO.”

Patch for the Spatiam DTN technology demonstration on the ISS. Media Credit: Spatiam Corporation

Looking to the future, the ability to communicate and transfer data will be crucial for exploration missions across our solar system. However, these capabilities will also be invaluable to the astronauts on those missions. Connection and communication are a central part of our humanity. With the help of DTN technology, astronauts on the Moon and Mars may be able to chat with family and friends back on

Earth and send photos just as easily as we do today. And who knows—maybe one day, they'll even be able to enjoy their favorite music, TV shows, and movies, too.

"I feel like I'm at the beginning of a much longer novel," said Cerf, who is now in his 80s. "I won't see the end of it, but I don't regret that. I'm having too much fun being at the first few chapters and feeling like I have a front row seat for the evolution of a new capability that will one day serve humankind going off planet."

Quantum HyperSpace Project Could Secure $Billions in Transatlantic Data

July 15, 2025BY QUANTUM NEWS

Scientists are attempting to establish a secure, unhackable communication system across the Atlantic, building on over a century of wireless transmission advancements. The €15 million HyperSpace project, co-funded by the EU and Canada, unites researchers from seven institutions to overcome the limitations of fibre-optic quantum communication by utilising satellite-based transmission. Scheduled for completion this September, the initiative aims to demonstrate the feasibility of intercontinental quantum key distribution, potentially underpinning a future global quantum internet and secure data network.

Quantum Communication's Transatlantic Ambition

The HyperSpace project represents a renewed ambition to establish transatlantic communication, albeit predicated on fundamentally different principles than those employed by Marconi. Rather than relying on radio waves, the initiative seeks to create a system of quantum secure communication, leveraging the principles of quantum mechanics to guarantee the inviolability of transmitted data. While a fully functional transatlantic link remains a considerable undertaking, the project aims to resolve the key scientific and technological challenges obstructing such a breakthrough.

At the core of this endeavour lies quantum entanglement, a phenomenon whereby two or more particles become linked in such a way that they share the same fate, irrespective of the distance separating them. This interconnectedness allows for the generation of encryption keys at a distance, offering a level of security unattainable through conventional cryptographic methods. Any attempt to intercept a quantum signal inevitably disrupts the entanglement, immediately alerting communicating parties to the intrusion and rendering the communication unusable to an eavesdropper.

Current quantum communication systems predominantly utilise fibre optic cables, but their range is limited by signal attenuation, typically extending to only a few hundred kilometres. To overcome this limitation, HyperSpace is investigating the feasibility of space-based transmission, exploring methods to relay quantum signals between satellites and ground stations. This approach promises to extend the reach of secure communication to intercontinental distances.

Furthermore, the HyperSpace consortium is exploring high-dimensional entanglement, a technique designed to increase the information-carrying capacity of individual photons. Unlike standard

entanglement, which transmits one bit of information at a time, high-dimensional entanglement allows for the simultaneous transmission of multiple bits, potentially increasing data transfer rates and bolstering the system's resilience against interference and hacking attempts.

The project's immediate focus is the development of a proof-of-concept system utilising shorter terrestrial free-space optical links, with the ultimate goal of establishing a secure quantum communication link between Europe and Canada. Success in this endeavour would not only demonstrate the viability of intercontinental quantum networks but also provide a blueprint for a future global system capable of supporting secure data sharing, precise navigation, and advanced computing applications.

The initiative benefits from a strong foundation in European quantum optics and photonic integration, crucial for scaling quantum communication technologies beyond laboratory settings and into operational spaceborne networks. Co-funded by the European Union's Horizon Europe programme and Canada's Natural Sciences and Engineering Research Council, the consortium brings together leading research institutions from across Europe and Canada, including Fraunhofer IOF, CEA-Leti, TU Wien, the Universities of Padua and Pavia, the Institut National de la Recherche Scientifique, the University of Toronto, and the University of Waterloo.

The Principles of Quantum Entanglement

The principle of quantum entanglement, central to HyperSpace, arises from the peculiar rules governing quantum mechanics. Unlike classical physics, where properties of an object are definite, quantum particles exist in a superposition of states until measured. Entanglement occurs when two or more particles become correlated in such a way that their fates are intertwined. Measuring a property of one particle instantaneously determines the corresponding property of the other, regardless of the distance separating them – a phenomenon Einstein famously termed "spooky action at a distance". This correlation is not due to any physical signal passing between the particles, but rather a fundamental property of their shared quantum state.

This interconnectedness is exploited in quantum secure communication by utilising the entangled particles to generate shared, random encryption keys. These keys are not transmitted directly, but are instead established through the measurement of the entangled particles. Any attempt by an eavesdropper to intercept or measure the particles disrupts the entanglement, altering the quantum state and immediately alerting the communicating parties to the intrusion. This inherent security is a critical distinction from conventional cryptography, which relies on the computational difficulty of mathematical problems and is therefore vulnerable to advances in computing power, including quantum computers.

The HyperSpace team is further investigating high-dimensional entanglement to enhance the efficiency and robustness of the system. Standard entanglement typically encodes information onto a single property of a photon, effectively transmitting one bit of information at a time. High-dimensional entanglement, however, leverages multiple degrees of freedom within the photon – such as its polarisation or orbital angular momentum – to encode multiple qubits simultaneously. This increases the information-carrying capacity of each photon, potentially boosting data transfer rates and improving resilience against noise and interference, ultimately strengthening the foundations of quantum secure communication.

Overcoming Distance Limitations

The limitations of terrestrial fibre optic networks necessitate the exploration of alternative transmission methods. HyperSpace is therefore focused on establishing quantum communication links via satellite relays, a complex undertaking requiring precise pointing and tracking of optical signals across vast distances. Maintaining the delicate quantum state of photons during transmission through the atmosphere and space presents significant technical challenges, including atmospheric turbulence, signal scattering, and photon loss. The project is investigating advanced adaptive optics and error correction protocols to mitigate these effects and ensure reliable data transmission.

Beyond simply extending the range of quantum communication, the HyperSpace consortium is actively researching techniques to increase the data throughput of these links. Standard quantum key distribution (QKD) protocols, while secure, often suffer from relatively low key generation rates. High-dimensional entanglement offers a pathway to overcome this bottleneck. By encoding multiple qubits onto a single photon – utilising properties beyond simple polarisation – the information-carrying capacity can be substantially increased. This not only accelerates key generation but also enhances the system's resilience against both interference and deliberate attacks, bolstering the integrity of quantum secure communication.

Successful implementation of space-based quantum communication will require not only technological advancements but also the development of standardised protocols and infrastructure. Establishing a globally interoperable quantum network will necessitate agreement on key distribution methods, data formats, and security standards. The HyperSpace project, by fostering collaboration between leading research institutions in Europe and Canada, aims to contribute to the development of these essential standards, paving the way for a future where quantum secure communication is readily accessible and widely deployed.

Enhancing Capacity with High-Dimensional Entanglement

The exploration of high-dimensional entanglement represents a significant advancement in enhancing the capacity of quantum communication systems. While standard entanglement schemes encode information onto a single quantum property – effectively transmitting one bit per photon – high-dimensional entanglement leverages multiple degrees of freedom within the photon itself. These degrees of freedom include, but are not limited to, polarisation, orbital angular momentum, and time-bin encoding. By exploiting these additional dimensions, each photon can carry multiple qubits simultaneously, substantially increasing the information-carrying capacity and potential data transfer rates. This approach moves beyond the limitations of single-bit transmission, offering a pathway to more efficient and scalable quantum secure communication.

Beyond simply increasing throughput, high-dimensional entanglement also offers inherent advantages in terms of robustness. Encoding information across multiple degrees of freedom diversifies the potential attack vectors. An eavesdropper attempting to intercept the quantum signal would need to simultaneously monitor and disrupt multiple, independent quantum states, significantly increasing the complexity and detectability of the attack. Furthermore, the increased

dimensionality provides greater resilience against noise and interference, as errors in one dimension are less likely to corrupt the entire message. This enhanced robustness is crucial for establishing reliable quantum secure communication links, particularly over long distances and through challenging atmospheric conditions.

The implementation of high-dimensional entanglement is not without its challenges. Maintaining the coherence of multiple quantum states simultaneously requires precise control and measurement techniques. Furthermore, the detection and decoding of high-dimensional quantum states often necessitate sophisticated optical setups and signal processing algorithms. The HyperSpace consortium is actively developing and refining these technologies, focusing on integrated photonic circuits and advanced quantum detectors. These advancements are essential for translating the theoretical benefits of high-dimensional entanglement into practical, deployable quantum communication systems, ultimately bolstering the security and efficiency of future networks.

A Collaborative European-Canadian Initiative

The initiative benefits from a strong foundation in European quantum optics and photonic integration, crucial for scaling quantum communication technologies beyond laboratory settings and into operational spaceborne networks. Co-funded by the European Union's Horizon Europe programme and Canada's Natural Sciences and Engineering Research Council, the consortium brings together leading research institutions from across Europe and Canada, including Fraunhofer IOF, CEA-Leti, TU Wien, the Universities of Padua and Pavia, the Institut National de la Recherche Scientifique, the University of Toronto, and the University of Waterloo.

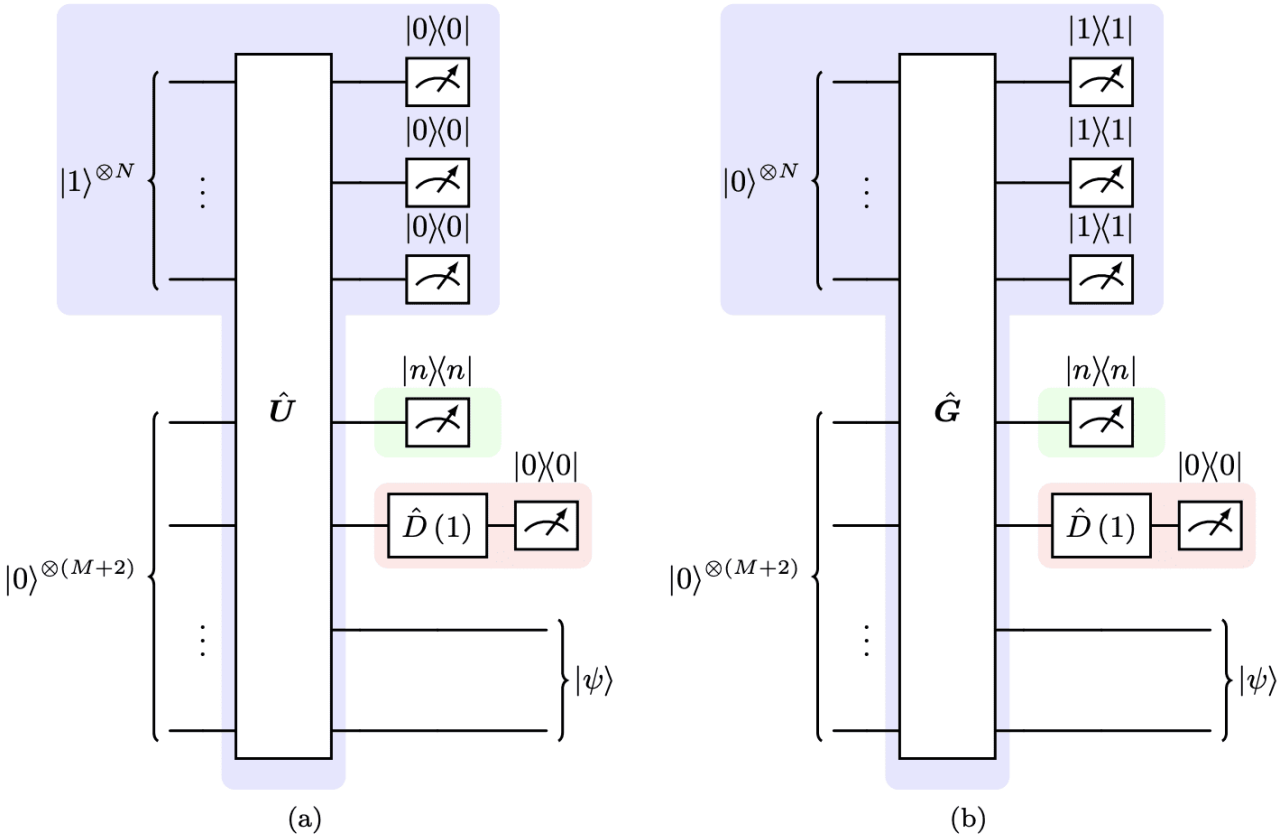
The HyperSpace consortium, concluding in September this year, comprises Fraunhofer IOF, CEA-Leti, TU Wien, the Universities of Padua and Pavia, and, from Canada, the Institut National de la Recherche Scientifique, the University of Toronto, and the University of Waterloo. This collaborative structure is intended to leverage complementary expertise in quantum optics, photonic integration, satellite communication, and free-space optical links, accelerating the development of essential technologies for intercontinental quantum secure communication.

Europe has established a strong lead in quantum optics and photonic integration, crucial for scaling quantum communications from laboratory experiments to spaceborne networks. This expertise is particularly relevant to the development of compact, efficient, and robust quantum transmitters and receivers, essential for deployment on satellites and ground stations. The Canadian contribution focuses on advanced free-space optical communication techniques and satellite mission design, complementing the European strengths in quantum photonics.

The consortium's collaborative approach extends beyond technological development to include the standardisation of protocols and infrastructure. Establishing a globally interoperable quantum network will necessitate agreement on key distribution methods, data formats, and security standards. The HyperSpace project, by fostering collaboration between leading research institutions in Europe and Canada, aims to contribute to the development of these essential standards, paving the way for a future where quantum secure communication is readily accessible and widely deployed.

Photonic States Engineered with Controlled Steps via Tensor Decomposition and Photon Catalysis

July 28, 2025BY QUANTUM NEWS



The creation of complex light states, essential for advances in quantum technologies ranging from computing to sensing, often presents significant challenges. Andrei Aralov from Laboratoire Kastler Brossel, alongside colleagues, now demonstrates a new method for generating these intricate states with precise control and a minimal number of steps. The team establishes a link between manipulating light and the mathematical problem of symmetric tensor decomposition, revealing a surprising ‘photon catalysis’ effect where photons are temporarily injected and retrieved to create entanglement beyond the reach of conventional techniques. This innovative approach, which also introduces a generalized tensor decomposition for designing optimal circuits, achieves perfect fidelity in simulations

across various light states, representing a substantial step forward in photonic quantum engineering.

Photonic quantum computing extends beyond computation to applications such as quantum sensing. This work presents a procedure for generating any desired quantum state exactly, and with a controlled number of steps. The method relies solely on multiport interferometers, photon number resolving detectors, photon additions, and displacements. Researchers achieve this goal by establishing a connection between photonic quantum state engineering and the algebraic problem of symmetric tensor decomposition, revealing a mechanism of photon catalysis where photons are injected and subsequently retrieved in measurements to generate entanglement unattainable through conventional means.

Quantum Optics, Tensors, and Machine Learning Tools

This extensive collection of research papers covers a broad range of topics including quantum optics, tensor decomposition, algebraic geometry, and machine learning. The bibliography focuses on continuous-variable quantum computation, exploring techniques to generate and manipulate squeezed states and non-Gaussian states for building quantum computers using light. A central theme is tensor decomposition and algebraic geometry, with a strong emphasis on understanding the mathematical foundations of quantum information. The inclusion of DeepMind's JAX ecosystem suggests an interest in applying machine learning tools to solve problems in quantum optics and improve computational efficiency.

The bibliography delves into specific areas such as low-rank approximations of tensors, algebraic geometry of tensors, and algorithms for tensor decomposition, alongside mathematical foundations including matrix analysis, projective geometry, and invariant theory. This suggests a desire to build a solid theoretical framework for the research, utilizing JAX for optimization algorithms and numerical linear algebra essential for working with tensors and matrices. This collection of resources points to several exciting research directions, including hybrid quantum-classical algorithms that use machine learning to optimize quantum state preparation and control, and tensor network methods for quantum simulation. Researchers are also exploring the application of algebraic geometry to understand the structure of quantum states and the limitations of quantum computation, developing new methods for generating non-Gaussian states using photon catalysis and designing scalable quantum architectures based on integrated photonics. Finally, it highlights the potential of tensor networks for quantum error correction and developing new algorithms for tensor decomposition with applications to both quantum information and machine learning.

Photon Catalysis Creates Complex Quantum States

Researchers have developed a new method for creating any desired multimode multiphoton state, a crucial resource for advanced quantum technologies like quantum

computing and sensing. These complex states, involving multiple photons distributed across multiple modes, are notoriously difficult to produce with precision using standard techniques. This new approach overcomes these limitations by connecting photonic state engineering with a mathematical concept called symmetric tensor decomposition. The team's method relies on a process akin to photon "catalysis", where photons are initially injected into a system and then retrieved during measurement, allowing for the creation of entanglement otherwise inaccessible through conventional means.

Importantly, the researchers demonstrate that their method can achieve 100% fidelity in generating these complex states, meaning the created states perfectly match the intended design, across a range of different configurations. This breakthrough addresses a long-standing challenge in the field, as previous methods were limited in the types of states they could produce. The new technique utilizes ancillary modes and photon counting to project the system into the desired state, offering a quantifiable cost and guaranteed fidelity. Furthermore, the researchers have shown that this approach can generate states with any number of photons distributed across the modes, including those with uneven distributions, expanding the possibilities for quantum applications.

The team has identified two potential implementations of this method, one using a specialized boson sampler and another utilizing a Gaussian boson sampler, both established photonic devices. While the boson sampler requires seeding with a larger number of photons, these are ultimately retrieved, serving the crucial purpose of creating the necessary entanglement. The Gaussian boson sampler implementation involves injecting weakly squeezed states into an interferometer, a technique already used for creating single-mode non-Gaussian states, but now extended to the multimode case. This work provides the first explicit demonstration of a general quantum state-engineering protocol, offering a powerful new tool for researchers developing future quantum technologies.

Multimode States from Interferometers and Detectors

This research presents a new method for creating arbitrary multimode multiphoton states, essential resources for various photonic technologies. The team successfully demonstrated a procedure to generate these states using only multiport interferometers, photon additions, photon subtractions, and photon number resolving detectors, establishing a link between photonic state engineering and symmetric tensor decomposition. Numerical evaluations confirm the method achieves 100% fidelity for different classes of states, suggesting it provides a bound on the resources needed for state preparation. While not optimal for all specific state types, and with computational limitations for very large states, the generality of this approach offers a valuable tool for quantum optical experiments. The authors acknowledge that determining the minimal number of "catalysis" photons required for state preparation and extending the method to mixed states represent areas for future investigation, alongside exploring refinements to achieve higher success probabilities and generalizing the core theorem to incorporate unitary transformations, potentially leading to more feasible designs for continuous-variable quantum information processing. This

research highlights a connection between the decomposition rank and entanglement properties, opening avenues for further theoretical exploration.

👉 **More information**

✏ *Photon catalysis for general multimode multi-photon quantum state preparation*

Quantum internet moves closer as researchers teleport light-based information JULY 21, 2025

by Ingrid Fadelli, Phys.org edited by Gaby Clark, reviewed by Andrew Zinin

Quantum teleportation from telecom photons to erbium-ion ensembles. Credit: Group of Prof. Xiao-Song Ma at Nanjing University.
Quantum teleportation is a fascinating process that involves transferring a particle's quantum state to another distant location, without moving or detecting the particle itself. This process could be central to the realization of a so-called "quantum internet," a version of the internet that enables the safe and instant transmission of quantum information between devices within the same network.

Quantum teleportation is far from a recent idea, as it was experimentally realized several times in the past. Nonetheless, most previous demonstrations utilized frequency conversion rather than natively operating in the telecom band.

Researchers at Nanjing University recently demonstrated the teleportation of a telecom-wavelength photonic qubit (i.e., a quantum bit encoded in light at the same wavelengths supporting current communications) to a telecom quantum memory. Their paper, published in *Physical Review Letters*, could open new possibilities for the realization of scalable quantum networks and thus potentially a quantum internet.

"Quantum teleportation is always a fascinating protocol in quantum communication for its ability to transfer quantum states without ever revealing," Xiao-Song Ma, senior author of the paper, told Phys.org. "To extend the state transmission distance further, the incorporation of quantum memory into a quantum teleportation system is of critical importance."

The main objective of the recent study by Ma and his colleagues was to successfully integrate a telecom solid-state quantum memory into a quantum teleportation system, which would enable the storage of transmitted quantum information. The main role of this memory would be to spread and store entangled particles across a quantum network (i.e., entanglement distribution).

Quantum networks rely on quantum repeaters, devices that can break the distances across which information is transmitted into shorter and more manageable sections, known as elementary links. When placed at the end of these sections, quantum memories could store quantum information for the time necessary for entanglement to be established across entire segments of networks, which could in turn enable its transmission across longer distances.

"We employed five systems to accomplish the experiment," explained Ma. "These include an Input state preparation; an EPR-source to generate entangled photon pairs from an integrated photonic chip, a Bell-state measurement and a quantum memory based on erbium ion ensembles. We also employed a frequency distribution and fine-tuning module based on an F-P cavity and PDH technique."

This recent work by Ma and his colleagues shows that quantum information could be transferred across a network using devices and optical wavelengths that are compatible with those currently employed in communications. The team's demonstration of quantum teleportation could inform the advancement of quantum networks, potentially contributing to the future realization of a reliable quantum internet.

"Our study demonstrated the quantum teleportation from telecom photons to a solid-state quantum memory based on erbium ions for the first time," added Ma. "Our entire system uses components compatible with existing fiber networks perfectly. This telecom-compatible platform for generating, storing and processing quantum states of light establishes a highly promising approach to large-scale quantum networks."

As part of their next studies, the researchers plan to focus on improving the performance of the erbium ion-based solid-state memory employed in their experiments. More specifically, they would like to extend its storage times and improve the efficiency with which it stores quantum information.

More information: Yu-Yang An et al, Quantum Teleportation from Telecom Photons to Erbium-Ion Ensembles, *Physical Review Letters* (2025). DOI: 10.1103/3wh8-2gh1.
Journal information: Physical Review Let