Located at the Swiss National Supercomputing Centre (CSCS), in Lugano, Piz Daint is being used to parse huge data sets and simulate processes for projects in geophysics, materials science, chemistry, and other areas, but especially in climate modeling. To power that research, the computer uses a hybrid system that combines the advanced network architecture of the Cray XC30 with two cutting-edge processors, the Intel Xeon E5 CPU and the Nvidia Tesla K20X GPU. The computer's 5272 compute nodes are bound together in a special low-latency network to form an unusually compact machine. Thomas Schulthess, the director of CSCS, says that Piz Daint uses 28 cabinets to achieve what would take 50 cabinets of the second most powerful computer in the world, Titan, which Schulthess worked on at Oak Ridge National Laboratory, in Tennessee.

But the supercomputer's real secret is that whenever possible its software keeps data from having to travel between processors. "What we really wanted on Piz Daint was to motivate users to consider how they organize their data in applications," says Schulthess. He thinks that optimizing where data resides relative to where it's computed and improving how multiple simultaneous computations can be performed on the same set of data "are the two ingredients to our future algorithms and application design."

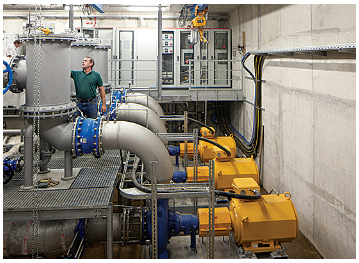
Applications that run on Piz Daint, which is named for a mountain in the Swiss Alps, use custom algorithms that intentionally position large data sets for processing on either the GPU or the CPU so the data won't have to be moved much or reconfigured later on. These efficiencies speed computing, because Piz Daint isn't taking time to locate and cull data. They also decrease energy consumption, by reducing data movement between processors and even within one processor in the case of the GPUs.

The machine needed to be built in two steps because the team had to wait for supercomputer manufacturer Cray to release the hybrid version of the XC30 architecture. But Schulthess says this was almost preferable because it gave the CSCS group time to do extensive testing on the smaller network and iron out any kinks before adding the XC30 to create the hybrid system in October.

It was worth the effort. "It's bad to say as an engineer when you're surprised, but Piz Daint in the end was so energy efficient, it was actually better than we expected," Schulthess says.

Feng hopes that Piz Daint's success will encourage other research groups to be more aware of their supercomputers' carbon footprints. This would be a step toward "simulating the climate, not generating it," he says.

—LILY HAY NEWMAN



WATER VERSUS WATTS: The Swiss supercomputer is cooled by water from nearby Lake Lugano.

NSA SURVEILLANCE SPARKS TALK OF NATIONAL INTERNETS

Germany takes the lead in making the Internet local

Just imagine the "network of all networks," the globe-spanning Internet, becoming a loose web of tightly guarded, nearly impermeable regional or even national networks. It seems antithetical to the mythology surrounding the Internet's power and purpose. But ongoing revelations about the extensive surveillance activities of the U.S. National Security Agency (NSA) are pushing countries like Germany and Brazil to take concrete steps in that direction.

Within the 28-member European Union, Germany is taking the lead in pushing for measures to shield local Internet communications from foreign intelligence services. That should come as no surprise. For Germans from the formerly Communist-ruled part of the country, NSA spying sparks bitter memories of eavesdropping by the Stasi, the secret police agency of the former East Germany. Because of that history, Germany has one of the strictest data privacy regimes in the world. On more than one occasion, the country has forced Google and other Internet companies to amend their data collection and usage practices.

For German chancellor Angela Merkel, the revelations are particularly disturbing: The political leader, who grew up under Stasi scrutiny, has had to deal with allegations that her own mobile phone was tapped by the NSA. She's not amused.

"Cybersecurity is no longer a niche topic but a top priority," Deutsche Telekom CEO René Obermann told attendees of the Cyber Security Summit late last year, in Bonn. He noted that his company battles more than 800 000 attacks a day on its networks.

MARCO CAROCARI

WHO IS LISTENING? German chancellor Angela Merkel was shocked to learn that the U.S. National Security Agency had been tapping her phone. Germany is considering steps to guard its network.

JOCK FISTICK/BLOOMBERG/GETTY IMAGES

A number of policymakers in Berlin and the country's network regulator back Deutsche Telekom's efforts to tighten security through "national routing," says Obermann. Essentially, the concept aims to handle data generated in Germany and destined for or used by local end users by means of fiber-optic cables, routing gear, and computers within the country. The aim is to avoid sending data packets through nodes in the United States and the United Kingdom. The operator, which already offers an encrypted "Made in Germany" e-mail service and cloud service, has also suggested expanding the idea to include all 26 countries participating in the borderless Schengen Area in Europe. Deutsche Telekom already carries much of the Internet traffic in Germany via reciprocal, or peering, agreements with ISPs, with the remainder handled by an array of operators, many of them foreign-owned.

The kind of segmenting of Internet communications Obermann is talking about would require operators to have two essential components: a national peering agreement that links the Internet networks of all the service providers; and a routing table, also known as a routing information base (RIB), that describes the topology of the networks. Routing tables maintained by the operators currently contain no instructions to keep in-country packets inside the country. The operators would also need their own German-specific routing protocols, which set down how the routers communicate with each other.

Deutsche Telekom claims it has the technology and know-how and needs just three more peering agreements to be able to provide such national routing. The operator, which is also open to the idea of forming a national routing entity, says more than two-thirds of its e-mail traffic is generated and terminated in Germany, and it is pushing parliamentarians to make the needed agreements mandatory.

European governments aren't the only ones looking to break off from what they see as American control of the Internet. The Open Root Server Network (ORSN) is an alternative network of domain name servers—machines that translate the names of Web addresses into the numbers of Internet addresses. Originally established to counter the fact that most of the domain name servers were in the United States at the turn of the 21st century, it operated from 2002 to 2008, when an expansion of the domain name server system made it defunct. But following ex-NSA contractor Edward Snowden's revelations about the agency's spying, the ORSN has been revived. "We're detached from a single country, like the U.S., which still controls" the Internet Corporation for Assigned Names and Numbers, says Markus Grundmann, one of the network's founders and coordinators.

Beyond Europe, Brazil's president, Dilma Rousseff, is one of the most outspoken heads of state to criticize NSA practices and take action. She is pushing legislation to force Internet companies such as Google and Facebook to store local data within the country's borders. She also wants to build submarine cables that don't route through the United States, set up domestic Internet exchange points, and create an encrypted national e-mail service.

International operators keen to implement some sort of national or regional routing are quick to point out that the practice already exists in the United States. Nationally generated and terminated traffic is prohibited from being routed over nodes outside the country. Foreign carriers with operations in the country must sign a compliance agreement.

But is a Brazilian lockdown or a German "Internetz," as the local media are calling it, the answer to preventing state-sponsored spying and hacking? Many industry experts have their doubts.

"A balkanization of the Internet is not the solution and runs totally contrary to the basic principles of the Internet," says Norbert Pohlmann, president of the German IT security association TeleTrust. He points to the Internet's ability to take advantage of global cost and capacity opportunities to route traffic.

Leslie Daigle of the Internet Society writes that the Internet "was not designed to recognize national boundaries" but rather for resiliency, which is "achieved through diversity of infrastructure: Having multiple connections and different routes between key points ensures that traffic can route around network problems and nodes that are off the air because of technical, physical, or political interference, for example."

That said, Pohlmann argues that the Internet community still needs "a common global infrastructure that ensures a high level of IT security, even if no one can guarantee 100 percent security." He calls on users to rely on end-to-end encryption and virtual private networks, which would make spy-agency snooping difficult.

But Jacob Appelbaum, a developer of the Tor Project, warns that even secure systems like virtual private networks can be rendered useless through misuse of so-called backdoors. Backdoors are essentially software designs in networks that allow authorities to conduct "deep packet" inspection to monitor and intercept data. The European Telecommunications Standards Institute, for instance, works closely with operators, government, and law enforcement agencies to integrate surveillance capabilities into communications networks. But many operators are concerned about how access to the backdoor "keys" is regulated, and, in the case of some equipment vendors—notably China's Huawei Technologies Co.—about whether secret backdoors are built into network systems without operators' knowledge.

Deutsche Telekom's Obermann acknowledges the problem. "We need strong and secure networks in Europe," he says. "Maybe that means we need to make the technology ourselves, or that the technology we buy doesn't provide backdoors."

But don't expect intelligence forces to ever give up trying to penetrate security systems, no matter how advanced they may be, cautions Neelie Kroes, vice president of the European Commission, which is responsible for Europe's digital agenda. "Spying is the world's second oldest profession," she said in Bonn. "Let's not be naive—it won't ever stop. We just need to be able to protect ourselves better." —JOHN BLAU

NEW PROBES REPLACE SURGEONS' SENSE OF TOUCH

Laparoscopic pressure sensors make 3-D maps of tumors

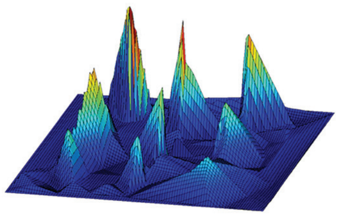
Surgeons' best tools for locating tumors inside the body are often their hands. But during minimally invasive surgeries—which can reduce recovery time by days—the ability to examine tissue through touch, called palpation, is lost. Instead, surgeons must manipulate the tissue with long, narrow instruments and rely on visual images from tiny cameras. But engineers in the United States, the United Kingdom, and elsewhere have designed new tools to help restore a surgeon's sense of touch.

The devices, dubbed palpation probes, are designed to be used laparoscopically and can detect changes in the stiffness of tissue. Tumors are harder than normal tissue, so they can be detected with a combination of pressure sensors and spatial positioning measurements. The readings are used to create a three-dimensional stiffness map that shows surgeons the margins of tumors.

A team at Nashville's Vanderbilt University led by biomechatronics engineer Pietro Valdastri showed *IEEE Spectrum* a wireless probe that a surgeon can manipulate in the body with a laparoscopic tool. The small, cylindrical prototype was banged up and wrapped in tape, looking more like something you might find on the floor of your garage than in a surgical suite. But it's what's inside that counts—a pressure sensor, a three-axis accelerometer, a three-axis magnetic field sensor, a battery, and a wireless microcontroller.

It works like this: The capsule's pressure-sensing tip is used to gently indent the tissue. The magnetic field sensor and accelerometer track the depth of the indentation, along with its position relative to a stationary magnet nearby. Each point of contact transmits information about the stiffness of the tissue at that point. Using an algorithm to fill in any unexplored area, the computer creates a 3-D color-coded map that displays the tumors. Valdastri's team has been testing their probe on a pig's liver and on a chunk of synthetic tissue that contains tumorlike lumps.

In the pig liver test, Valdastri's probe was off by just 8 percent in its stiffness measurement. "This new sensor capsule is quite successful in measuring tissue properties," says Robert Howe, a professor of engineering at



TUMORS ARE TOUGHER: In a stiffness map of a silicone sample, mock tumors stick out. Doctors could generate and use such maps during minimally invasive surgery.

STORM LAB