To look it of evil technology available worldwide. Some of them are incredibly powerful and sophisticated. Cybercrime may be on the rise, but conventional bugs are booming, as their "tools". From high-end optical detectors, video endoscopes to semiconductor frequency spectrum analyzers to acoustic vibrations through windowpanes. And then to use an infrared laser to decrypt sound waves across even greater distances.

That's quite an achievement," reported Jens Bolte, a countersurveillance expert, one of only two "publicly trained spies" in Germany. "That includes high-frequency measurements in wire- and acoustic spaces that can shelter audio or video devices powerful enough for espionage. The tip of a ballpoint pen cartridge, for instance, can be used to scribble secret messages that are only readable under a microscope. The specialists turn on a camera and record the image, which is then analyzed by a computer to decode the coded message.

"It's an art all its own," Bolte said. "We don't need a whole team to do it. Just a single person can achieve it." The experts work in a small room with a round table and a large window. They are looking for hidden cameras and microphones installed by spies. "It's an art all its own," Bolte said. "We don't need a whole team to do it. Just a single person can achieve it."

Deutsche Telekom's countersurveillance teams move out in groups of four or five. One of them, Horst Glaser, is a 62-year-old countersurveillance expert who has been with the company for nearly 40 years. He was a former German Army soldier who was trained as a countersurveillance expert. Deutsche Telekom has been offering technical surveillance countermeasures as a service to customers for nearly 40 years, too. Deutsche Telekom has its own quality management system (QMS), which is audited by the BSI, the German Federal Office for Information Security. To obtain this certification, a service provider must have implemented an audited quality management system (QMS), have a security clearance up to the level of "secret" and, as the government agency puts it in official documentation, "employees who are prepared to be exposed to an attack by potential attackers" as well as excellent skills in radio and communications.

The ability to put together such a highly qualified team is a big reason why Deutsche Telekom is the first – and so far the only – IT security service provider to offer "Technical Surveillance Countermeasures for the Private Sector" as certified by the BSI. Deutsche Telekom has become the "global expert" in this field and is able to offer a "complete solution" to its customers. The countersurveillance team is "fully prepared to handle any kind of security threat," Bolte said. "We can handle everything from breaking into a building to hacking into a computer system."
“unique identification number and cannot be removed through Wifi at a later time,” Horst Glaser explained. The active bugging devices that often send the information penetrate steel up to 1.6 inches thick.

The surveillance team’s toolkit includes semiconductor detection displays as a dark-red spot. Other tools in the counter-surveillance world are as varied as the criminals, and they require an equally nascent approach. The teams are trained to immediately alert the defense experts. The special equipment the team offers its customers is a conference support service. A spectrum analyzer will register transmissions in frequencies used by cell phones or tablets.

Once a room has been secured, the countersurveillance team can arrive at a customer’s site depending on the customer’s security policy. One important aspect is physical access control for specific rooms: who is authorized to clean the room or perform planned catering and equipment, floor, ceiling and wall construction, time of day or night, and weekend or business hours. A comprehensive sweep, i.e. an office measuring up to 30 square meters, includes a non-intrusive assessment of the security policy. The cost of a counter-surveillance audit can only be calculated in relation to the size of the space and the number of devices.

The team offers its customers a conference support service. A spectrum analyzer will register transmissions in frequencies used by cell phones or tablets. One aspect is physical access control for specific rooms: who is authorized to perform cleaning or equipment services? What’s the point of sweeping a room if the cleaning is done by people who are not authorized to enter the meeting room? How can you make sure they go as they please until the scheduled meeting finally takes place and they get away with the second strategy, which was an employee or used an employee’s hardware. Only then will the team offer a comprehensive sweep of the radio frequencies at the start of the meeting, followed by a constant comparison scan in the next room during the entire meeting. This allows them to detect the presence of any active bugging devices.

The team offers its customers a conference support service. A spectrum analyzer will register transmissions in frequencies used by cell phones or tablets. The cost of a counter-surveillance audit can only be calculated in relation to the size of the space and the number of devices.

The team offers its customers a conference support service. A spectrum analyzer will register transmissions in frequencies used by cell phones or tablets. The cost of a counter-surveillance audit can only be calculated in relation to the size of the space and the number of devices.