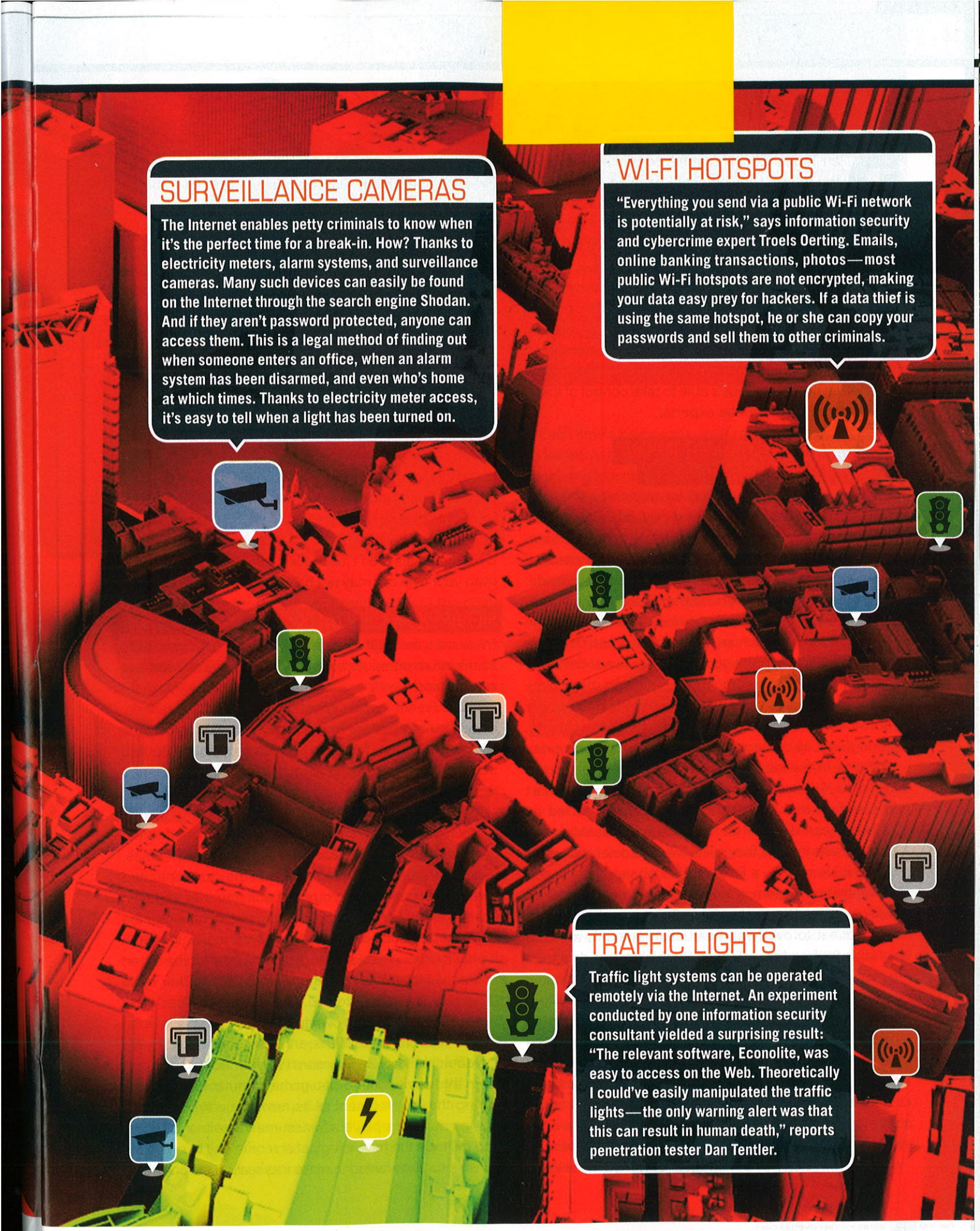
POWER PLANTS

They are surrounded by high fences; hundreds of security cameras monitor every inch of the site—yet power plants are often extremely vulnerable. The one thing many companies don't do enough to protect: the Internet. Most industrial facilities are connected to the Internet and their operations can be monitored and controlled remotely. If the interface with things like water pumps or cooling systems is open or secured by a simple password, hackers could easily penetrate the system and proceed to cause chaos.

CAN YOU HACK AN ENTIRE CITY?

Traffic lights, surveillance cameras, and power plants—nowadays billions of different systems are controlled via the Internet. The problem: It can take as little as a few minutes to infiltrate them and then take control of the infrastructure of a city...



SURVEILLANCE CAMERAS

The Internet enables petty criminals to know when it's the perfect time for a break-in. How? Thanks to electricity meters, alarm systems, and surveillance cameras. Many such devices can easily be found on the Internet through the search engine Shodan. And if they aren't password protected, anyone can access them. This is a legal method of finding out when someone enters an office, when an alarm system has been disarmed, and even who's home at which times. Thanks to electricity meter access, it's easy to tell when a light has been turned on.

WI-FI HOTSPOTS

"Everything you send via a public Wi-Fi network is potentially at risk," says information security and cybercrime expert Troels Oerting. Emails, online banking transactions, photos—most public Wi-Fi hotspots are not encrypted, making your data easy prey for hackers. If a data thief is using the same hotspot, he or she can copy your passwords and sell them to other criminals.

TRAFFIC LIGHTS

Traffic light systems can be operated remotely via the Internet. An experiment conducted by one information security consultant yielded a surprising result: "The relevant software, Econolite, was easy to access on the Web. Theoretically I could've easily manipulated the traffic lights—the only warning alert was that this can result in human death," reports penetration tester Dan Tentler.

Dan Tentler is sitting at his computer, searching the Internet for potential hacking victims. His mission: The information security consultant is attempting to ascertain how well our cities are protected against cyberattacks. How easy is it to switch the traffic light colors? How secure are our power plants? And how easy is it to manipulate technical equipment in a hospital? To answer these questions, Tentler doesn't require highly sophisticated hacker tools—all he needs is the search engine Shodan. It searches specifically for devices that are connected to the Internet. Then Tentler tests to see how quickly he's able to take control of them. The results shock even the experts...

WHY ARE FACTORIES BEING CONTROLLED REMOTELY?

Most computer systems used for private business or public infrastructure can be operated at considerable distances using software called SCADA (supervisory control and data acquisition). The upside: It's cheaper than sending an engineer to a given site. The downside: Many SCADA systems are not sufficiently protected. Even some major corporations don't bother to change default passwords such as 1234. Hackers can therefore easily access the operating system by way of the Web, enabling them to see company secrets and manipulate production processes. It only took security researcher Paul McMillan 16 minutes to find 30,000 open systems, although not all of them were from corporate networks.

Billions of devices worldwide are connected to the so-called "Internet of Things": More and more smart devices have their own IP address and are controlled via the Web. According to the investigations of McMillan and Tentler, these include things like two hydroelectric power plants in New York, a French wind power station, and the ventilation system of a Romanian mine. "You could easily manipulate an industrial boiler or a cooling system and cause it to overheat. Instruction manuals are also available for free," says Tentler. Such plans are designed to help engineers as they remotely operate the facilities. If these fall into the wrong hands, it's akin to serving a dangerous cyberweapon to a criminal on a silver platter.

If someone can make a power plant overheat, he also has the power to kill hundreds of people and cripple a small city's energy supply. If someone were to hack into a hospital's network, he could commit a perfect murder. Information security expert Scott Erven says it is even possible to control the administration of painkillers by way of an infusion pump managed remotely via the Web. To outsiders a murder by morphine overdose would look like a tragic accident. Only the hacker would know better.

CAN YOU TURN OFF SPEED CAMERAS?

But SCADA systems can also be manipulated to cause traffic chaos on the streets. When Tentler tried to access the license plate recognition system Autoplate, which is how those caught by speed cameras receive a ticket in the mail, he didn't even need a password. "You can hack into the system and tell it to send the photos to someone besides the police," he says. In Moscow, an unidentified cybercriminal shut down thousands of speed cameras in January 2014. "He infiltrated the isolated network and ruined all the systems. It was weeks before the cameras were up and running again," says Vitaly Kamluk of the IT security firm Kaspersky Lab. During that time, drivers were able to race through the city with no regard for the speed limit. However, what many motorists don't know: Cybercriminals aren't just hacking the speed cameras—even your own car may not be safe from a hack attack...

HOW DO YOU HACK INTO A CAR?

"New cars are built like a smartphone. They have 30 to 70 miniature computers that use four or five networks to communicate with one another and with the Internet," explains French hacker Jonathan Brossard. The reason: If you want to get the latest traffic information on your navigation device, for example, you have to connect to the Internet through an external service provider—and this kind of communication makes your car vulnerable. "In tests with one car manufacturer, my team managed to hack into a car from the outside through its Internet connection," says Brossard. He is not naming names, but he will say this: "Every network in the car is operated by a microcontroller. If you can hack into that and gain access to the car's control network, you could open the doors at the touch of a button, for instance." In general: If a car has been hacked into, it's game over for the driver. "Some vehicles have remote keyless entry. Their code can be captured and copied onto a blank key fob," says Brossard. Although the owner would still be able to open his car with his state-of-the-art radio-controlled key, so too could the hacker. Brossard is a member of an expert team that advised the video game manufacturer Ubisoft during the development of its new game *Watch Dogs*. The game allows players to assume the role of a hacker and infiltrate the technology of an entire city to complete a mission. "We wanted to make it as realistic as possible,"