Chapter 13 talks about smart cities are the next frontier. Locate the article where a researcher gained control of Ettlingen, a smart city in Germany. Comment on the article.

Chapter 13: Home Hacked Home of the Future Crimes book emphasizes how the Internet of Things (IoT) has made exceptional improvements in the quality of life in general by transforming our ecosystem into smart cities. These cities exhibit a complete digital nature that is comprised of sensors, and various IoT enabled devices that seamlessly connect to the internet to allow both residents and utility companies (such as energy and water) to gather real-time data efficiently. However, with the facilities no longer separated from the internet (a method that was used before to keep them secure) due to IoT, the number of attacks targeting critical infrastructures hasn’t slowed down a bit. Instead, attackers have found extended points of entry to ruin the community’s life in general completely.

In order to show the seriousness of the security concern, the author mentions an event from July 2014 where a security researcher was able to gain control of the power supply of Ettlingen, a smart city in Germany using an exploit. He asserts that a hacker could have used the same exploit to turn off power, water, and gas. A corresponding article released in the same month indicates that the researcher, Felix Linder, was very close to shutting down the power supply of 40,000 people in Ettlingen through his simulated cyberattack. Linder revealed that it was elementary to gain access to the control room by hacking into the utility’s network through its IT grid. According to him, he could have switched off everything from power to water and gas. Hence, the managing director of the utility asserted that the experiment was a clear indication of how sensitive critical infrastructure is not well protected from threats.

The released article goes deeper into cyberattacks on infrastructure as being a major concern for utility companies, especially after the 2010 Stuxnet computer virus that was utilized by the U.S. and Israel to demolish Iran’s nuclear centrifuges. It also talks about other malware such as Trojan that can be used by hackers to cause damage considering the broad deployment of smart meters at Utilities. The article further discusses the vulnerabilities in these new devices, risk, and financial values that can arise due to hacking incidents. That being said, to comment on the article, the amount of damage that can be incurred due to attacks launched on critical infrastructures has actually increased significantly. Communities have also witnessed these attacks, and the attack vectors have also been changing. It is also becoming increasingly difficult to detect the presence of hackers in utility environments due to Advanced Persistent Threats (APTs). Unfortunately, while the majority of the IoT devices we have currently are still insecure, we still keep on adding more smart devices worsening the problem. As a result, I think it is safe to say that we are all living in fear.

Article: <https://www.businessinsurance.com/article/00010101/NEWS06/140719922/Smart-technology-could-make-utilities-more-vulnerable-to-hackers>