blogs.lse.ac.uk
http://blogs.lse.ac.uk/usappblog/2016/02/18/cybersecurity-weaknesses-threaten-to-make-smart-cities-more-costly-and-dangerous-than-their-analog-predecessors/

Cybersecurity weaknesses threaten to make smart cities more costly and dangerous than their analog predecessors.

Recent years have seen where we live – from our homes to our cities – increasingly connected via the Internet of Things. While this connectivity can have huge benefits, such as reduced energy costs and improved traffic safety, these systems can also be vulnerable to hacking and other cybersecurity threats, warns **Natalie Allen**. *She writes that city officials must ensure that security is built into smart city technologies as they are implemented rather than responding after a crisis has occurred.*

The Internet of Things (IoT) is already deeply embedded in cities, making them smarter and providing public officials with data and resources to make them more efficient and cost-effective. As the IoT continues to grow and its innovations improve city life and management, it's key for public officials to actively work on addressing the real security concerns that come with network connections while the IoT is in its infancy. The costs of ignoring the security risks posed by networked objects are high: fraud can remove efficiency gains and unguarded IoT technologies leave cities vulnerable to costly and/or dangerous digital attacks.

Broadly speaking, the Internet of Things is a network of interconnected physical objects that allows these items to collect and share data. In addition to city-level integration, these networked devices are being used in private homes, for instance Google's Nest thermostat uses sensors, weather forecasts, and your preferences to adjust your home's temperature to keep you comfortable and reduce your energy usage. Comparable to the way IoT technologies are improving city life, personal use of these networked devices can help cut costs and streamline your life. However, these personal benefits pale in comparison to the possible improvements that IoT devices can have, and have already had in cities. Smart grid technology can save cities millions, sensor networks can monitor noise and air quality, which allow police to respond to gun fire before it is reported and city officials to focus on re-routing traffic and other solutions in heavily polluted areas, while public transit, parking and waste collection can all be made more efficient through smart technology.

Similarly, the safety and security issues surrounding personal IoT devices are a magnitude smaller than the cybersecurity weaknesses that threaten smart cites. This is not to say that these concerns are not serious, sales of Nest's smart fire alarm had to be temporarily halted after it was discovered that they could be accidentally turned off through user motions, which could have had deadly implications. However, cybersecurity weaknesses at the city level could result in huge financial losses and leave our cities vulnerable to remote, malicious attacks. Beyond this, city officials are extraordinarily well positioned to combat these flaws and affect change in the way that a normal consumer is not. For these reasons, it is crucial to focus on what public officials can do to address cybersecurity concerns with the integration of IoT devices.

Hackers are why we can't have nice things

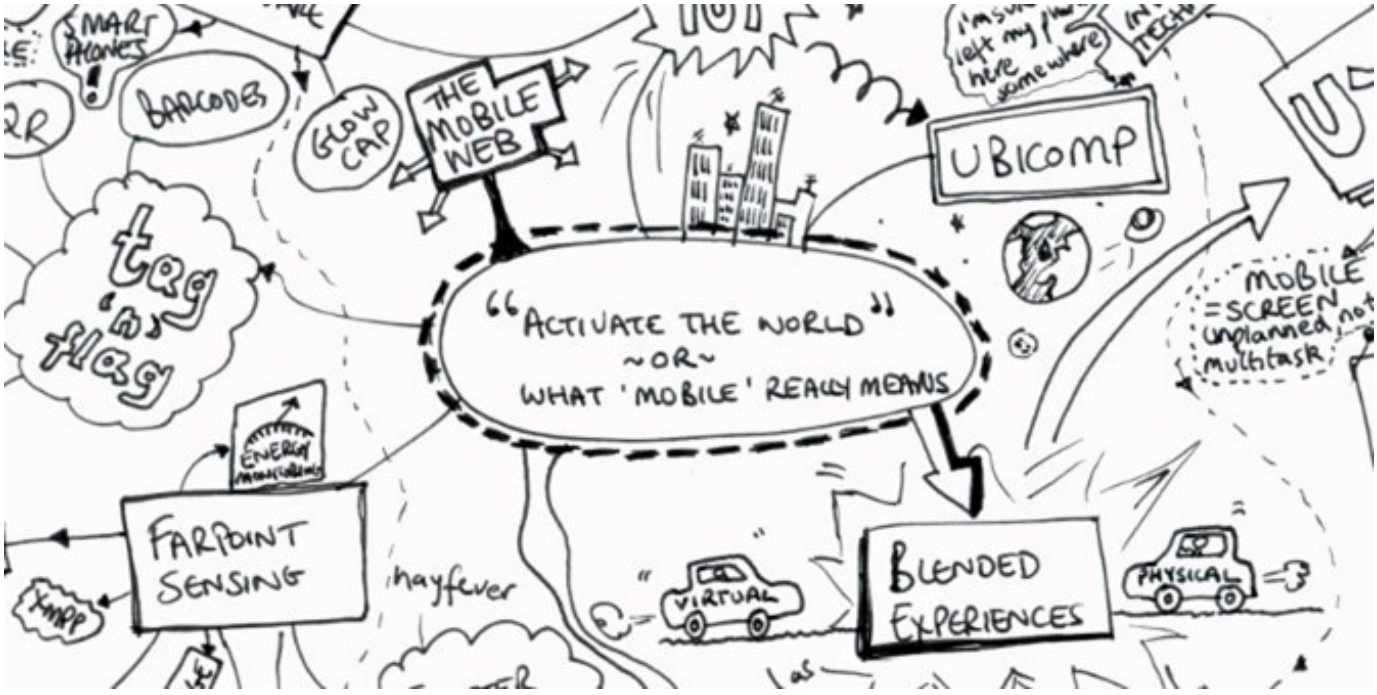
Insecurities within publicly used IoT devices have already been exploited in ways that affect both its efficacy and pose major risks to the public. In 2012, the FBI reported that an electrical utility company in Puerto Rico had asked for help after its smart meters, intended to improve efficiency across the electrical grid, were repeatedly hacked and reprogrammed to allow people to steal power or pay a significantly reduced rate. The FBI estimated that the losses from such smart meter fraud could cost the utility almost $400 million annually without accounting for negative externalities, such as increased pollution, that would accompany a rise in power consumption.

Fraud caused by hacking IoT technology creates serious inefficiencies that can ultimately be more costly than analog systems—exactly the opposite of the goal of smart cities. At best, this could make others hesitant to implement networked technologies. It could also lead cities to cease implementing or abandoning these highly beneficial technologies. While this would be a significant blow to progress, far more serious security issues in IoT technologies can actively threaten citizen safety.

Car accidents kill nearly 33,000 people in America each year, while many more are injured. IoT technologies that already exist or are currently being developed hold enormous promise for significantly reducing the number of auto accidents by using data and innovations like smart stoplights to better manage traffic flows, sensors that gauge where cars are in relation to other objects, and eventually the ability to eliminate human error altogether through driverless cars.

These technologies have already proven susceptible to security breaches, albeit with no serious consequences to date. This past summer altruistic hackers demonstrated car computers' vulnerabilities when they remotely took control of a Jeep Cherokee while it was on the highway and shut it down. Similarly, University of Michigan security researchers hacked into local traffic lights and were able to change their colors as they desired, while hacking road signs has become a beloved internet meme. It is not hard to imagine the chaos a malicious attack on this infrastructure could create.

We haven't seen any physical attacks yet, but unguarded IoT technologies have already played a hand in enabling digital attacks. Recently, 900 CCTV cameras around the world were used to carry out a denial of service (DDoS) attack. These cameras are easy to hack in part because many still think of them as cameras, rather than small computers. As a result, all of the offending devices were not properly secured, and were accessible through their default login credentials—something that would be unthinkable for a standard computer. In 2014, there were 245 million CCTV cameras operating throughout the world, with more coming online every day. DDoS attacks are costly, Kaspersky estimates that a single DDoS attack can cost a company between $52,000 and $444,000, and as IoT technologies become more widespread, they could become an invaluable resource to hackers if they are not properly secured.



Credit: Mike (Flickr, CC-BY-2.0)

So what do we do?

Given the threat an insecure Internet of Things poses to government, business, and citizens, direct and immediate action is needed while we are still in the early days of this technology. While many IoT technologies have already been incorporated into cities, the number of connections that currently exist is expected to more than quadruple by 2020. It is both easier and more efficient to build security into these technologies as they are implemented, rather than retroactively responding to a crisis.

Some city officials have already taken steps to ensure that smart technologies are properly secured. The mayor of Los Angeles, Eric Garcetti, signed an Executive Directive creating a Cyber Intrusion Command Center, in order to lead cybersecurity preparation and response efforts across city departments. All cities should follow this example and create similar centers, tasked with checking to ensure that all IoT enabled-technologies purchased by the city are designed with cybersecurity in mind, that these devices are installed properly, the incorporated software remains up to date, and that they are monitored for evidence of unusual activity. Plans and procedures should be preemptively put in place to isolate and remediate malicious software as it is detected.

Companies must also ensure that security is not an afterthought when creating and using smart technology. To date, many companies creating IoT devices have not made cybersecurity a priority, in large part because consumers currently care more about affordability and are often unaware of the security threat posed by insecure networked devices. Once again, this is often a result of an outdated mindset that thinks of their internet-enabled thermostat as a normal thermostat rather than a small computer. Efforts are currently being made the create a cybersecurity rating system for IoT devices to better inform consumers about the security of their devices, but cities are in a unique position to use their large buying power to shape the market. Similar efforts are already underway in San Francisco and other US cities to encourage gun safety by only purchasing firearms from “socially responsible” manufacturers who adhere to the city’s seven proof of practices.

The federal government has also taken steps to ensure IoT manufacturers take security into account, as the Federal Trade Commission (FTC) recently issued a set of best practices to “enhance and protect consumers’ privacy and security.” The FTC has also begun to prosecute cases against companies who have failed to secure their networked devices and it is not hard to imagine future lawsuits for negligence if consumers are harmed by a company’s failure to reasonably secure a car computer or similar device.

The IoT has already created real benefits in cities by arming officials with data and making city infrastructure more efficient, cost-effective and responsive. In the midst of all of these benefits, cities must keep an eye toward cybersecurity in order to prevent fraud from cutting into these gains, thwart costly digital attacks, and ultimately protect their citizens’ safety. These risks can be mitigated through ongoing and dedicated attention to security.

Please read our comments policy before commenting.

Note: This article gives the views of the author, and not the position of USAPP – American Politics and Policy, nor the London School of Economics.

Shortened URL for this post: **http://bit.ly/1Q33UTK**

About the author

Natalie Allen – *The Atlantic*

Natalie Allen received her MSc in Conflict Studies from the London School of Economics in 2014. While pursuing her degree, she also worked as an Assistant Editor on the LSE's USAPP blog. A 2013 graduate of Vassar College, Natalie is currently working as a production coordinator on the live events team for *The Atlantic*. She tweets at @nnallen on conflict, feminism, and Latin America.