# Nell’inferno delle cose connesse

Cosa rischiamo quando l’Internet delle Cose va più veloce delle pratiche necessarie a metterlo in sicurezza — e come invertire una tendenza che, incontrastata, porta dritti a scenari da distopia tecnologica

---

**Fabio Chiusi**

*Conferenza Nexa su Internet & Società, 2 dicembre 2016*

“The rush to connect everything to the Internet is leaving **millions** of everyday products vulnerable and ripe for abuse”

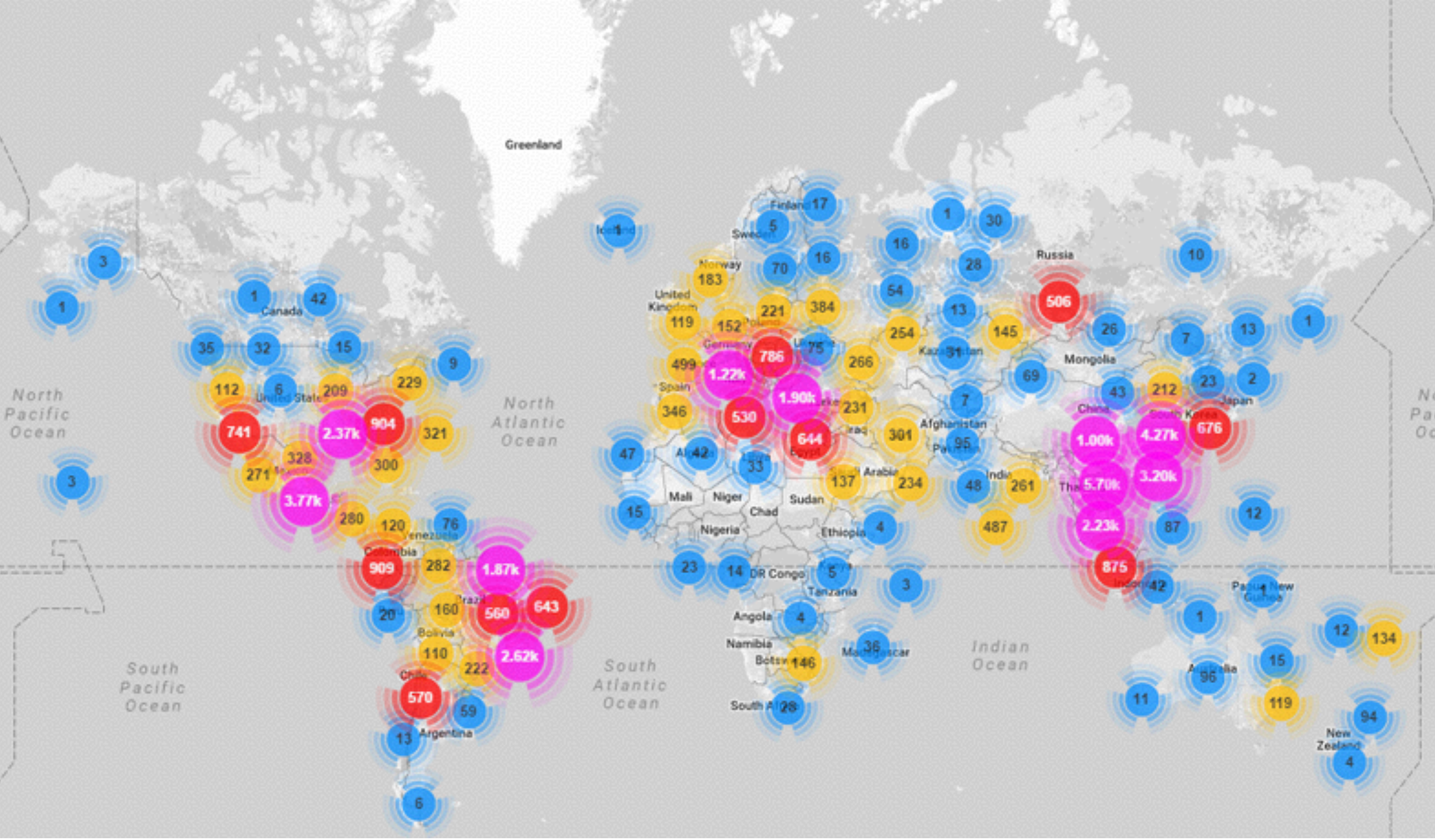
**– Level 3 Communications, *agosto 2016***

“Several recent reports have shown that some devices do not abide by **rudimentary** security and privacy best practices”

**– Broadband Internet Technical Advisory Group, ‘IoT Security and Privacy Recommendations’, *novembre 2016***

# *The gates of IoT hell*

- Si aprono il 21 ottobre 2016
- Airbnb, Amazon, BBC, CNN, Comcast, EA, Etsy, Guardian, GitHub, HBO, Imgur, NyTimes, PayPal, PlayStation Network, SoundCloud, Twitter, Yelp e molti altri vanno offline per ore
- Responsabile **una botnet di stampanti, videocamere, router, baby monitor** - IoT device reclutati da un malware di nome “Mirai” per attaccare Dyn. “Mirai”, in giapponese, significa “futuro”
- L’attacco DDoS a Dyn è il più potente finora mai visto: 1,2 terabit al secondo




# Eccolo, il “futuro”

“Mirai” è ormai diffuso in 164 paesi, dice Imperva. Sono 177 secondo MalwareTech.

# “Qualcuno sta imparando a spegnere Internet”

“Over the past year or two, someone has been **probing the defenses of the companies that run critical pieces of the Internet**. These probes take the form of precisely calibrated attacks designed to determine exactly how well these companies can defend themselves, and what would be required to take them down. We don't know who is doing this, but it feels like a large nation state. China or Russia would be my first guesses.”

- *Bruce Schneier, settembre 2016*

# Ma è solo l’inizio

- Il codice sorgente di “Mirai” è disponibile in rete, e chiunque può “affittare” botte da 400 mila oggetti connessi (Stati, organizzazioni criminali, hacker e hacktivisti)
- Ha già colpito il blog ‘Krebs on Security’ (con 1,5 milioni di device IoT) e la francese OVH (si parla di punte di 1,5 terabit/s)
- Ha provato a mandare offline l’intera Liberia
- Una sua evoluzione ha infettato 900 mila router broadband di Deutsche Telekom - lasciando **5 milioni** di device connessi in tutto il mondo insicuri: soprattutto in Germania, Brasile e UK, ma anche in Iran, Australia, Argentina, Turchia, e **Italia**.

“In this operation, the perpetrators have shown a high degree of skill. (…) Infrastructure of this scale is expensive and signifies not only that this is likely a commercial operation, but that there is an attempt to become **more resilient** to takedowns”

**– Flashpoint, *novembre 2016***

# Se tutto è connesso, tutto è *vulnerabile*

Perché l'innovazione in campo IoT è andata **più veloce** delle misure necessarie a rendere "sicuri" gli oggetti connessi

"While the benefits of IoT are undeniable, the reality is that **security is not keeping up with the pace of innovation**. As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats. Our increasing national dependence on network-connected technologies has grown *faster than the means to secure it*."

**- 'Strategic Principles for Securing the Internet of Things', US Department of Homeland Security, *novembre 2016***

# Una questione di sicurezza nazionale

"Last year, in a cyber attack that temporarily disabled the power grid in parts of Ukraine, the world saw the critical consequences that can result from failures in connected systems. Because our nation is now dependent on properly functioning networks to drive so many life-sustaining activities, **IoT security is now a matter of homeland security**" (*Id.*)

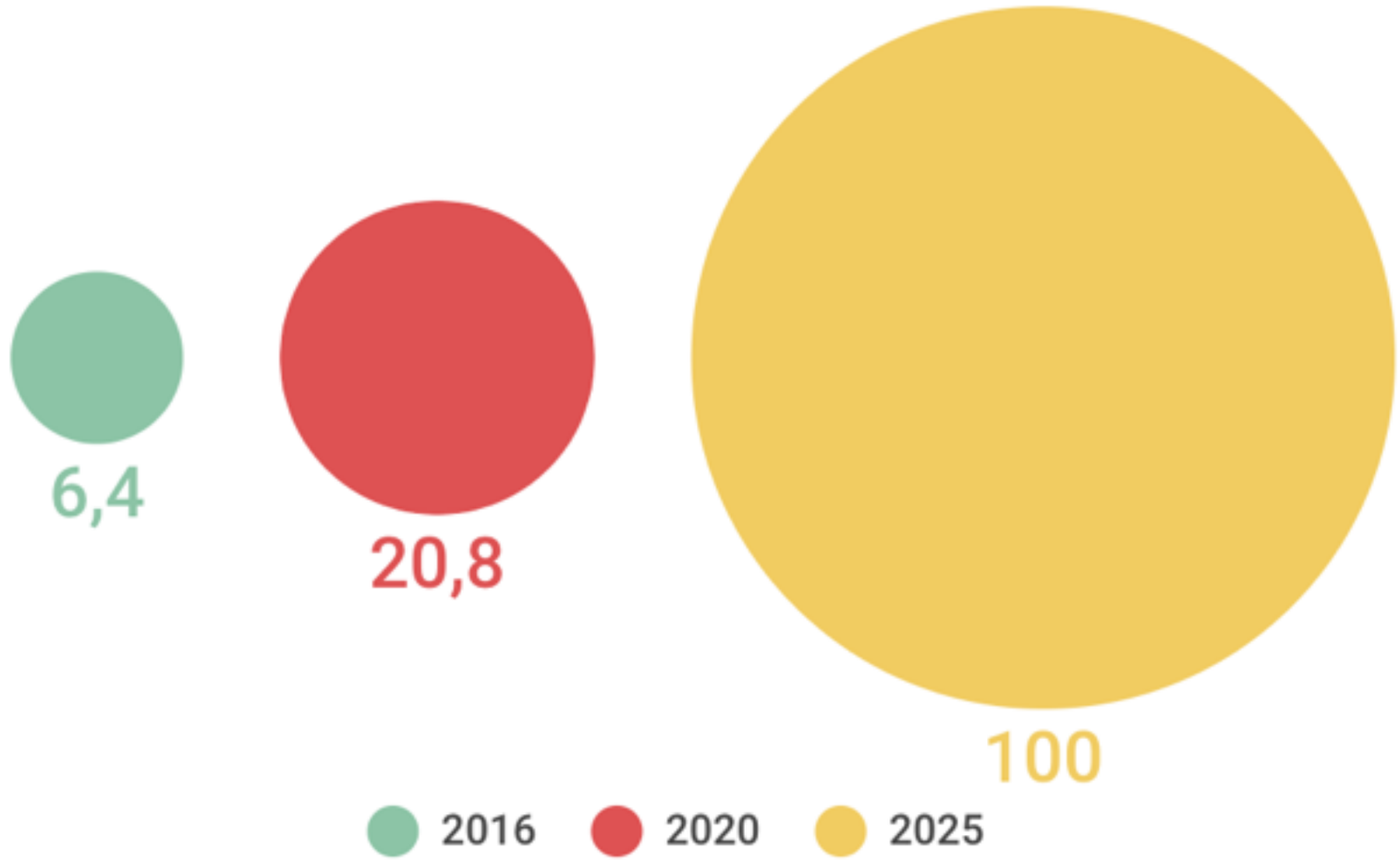
# Ma soprattutto, una questione che riguarda tutti

- Perché l'IoT è dappertutto, è il trend sarà *vertiginosamente* crescente secondo tutte le previsioni degli analisti di settore

- Già oggi sono *decine* i casi di hacking di device IoT insicuri **di uso quotidiano** che finiscono sul nostro corpo, nelle nostre case, negli spazi pubblici

- Dai trasporti alla salute, dal consumo energetico allo svago: ogni settore dell'umano diventerà *connesso*

# Miliardi di oggetti connessi




Le stime variano: Juniper dice 13,5 mld oggi, e 38,5 nel 2020

Fonti: Gartner, Huawei

# Frigoriferi *spammer*

Già nel 2014 un frigorifero connesso mandava mail di spam insieme ad altri 100 mila oggetti connessi manipolati da hacker; tra il 23 dicembre 2013 e il 6 gennaio la campagna ha mandato **750 mila mail di spam**, di cui il 25% è passato da smart tv, router domestici, elettrodomestici e altri device IoT

Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

If you do not enable Voice Recognition, you will not be able to use interactive voice recognition features, although you may be able to control your TV using certain predefined voice commands. While Samsung will not collect your spoken word, Samsung may still collect associated texts and other usage data so that

Behind Winston's back the voice from the telescreen was still babbling away about pig-iron and the overfulfilment of the Ninth Three-Year Plan. The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live--did live, from habit that became instinct--in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

**Parker Higgins**
@xor

Follow

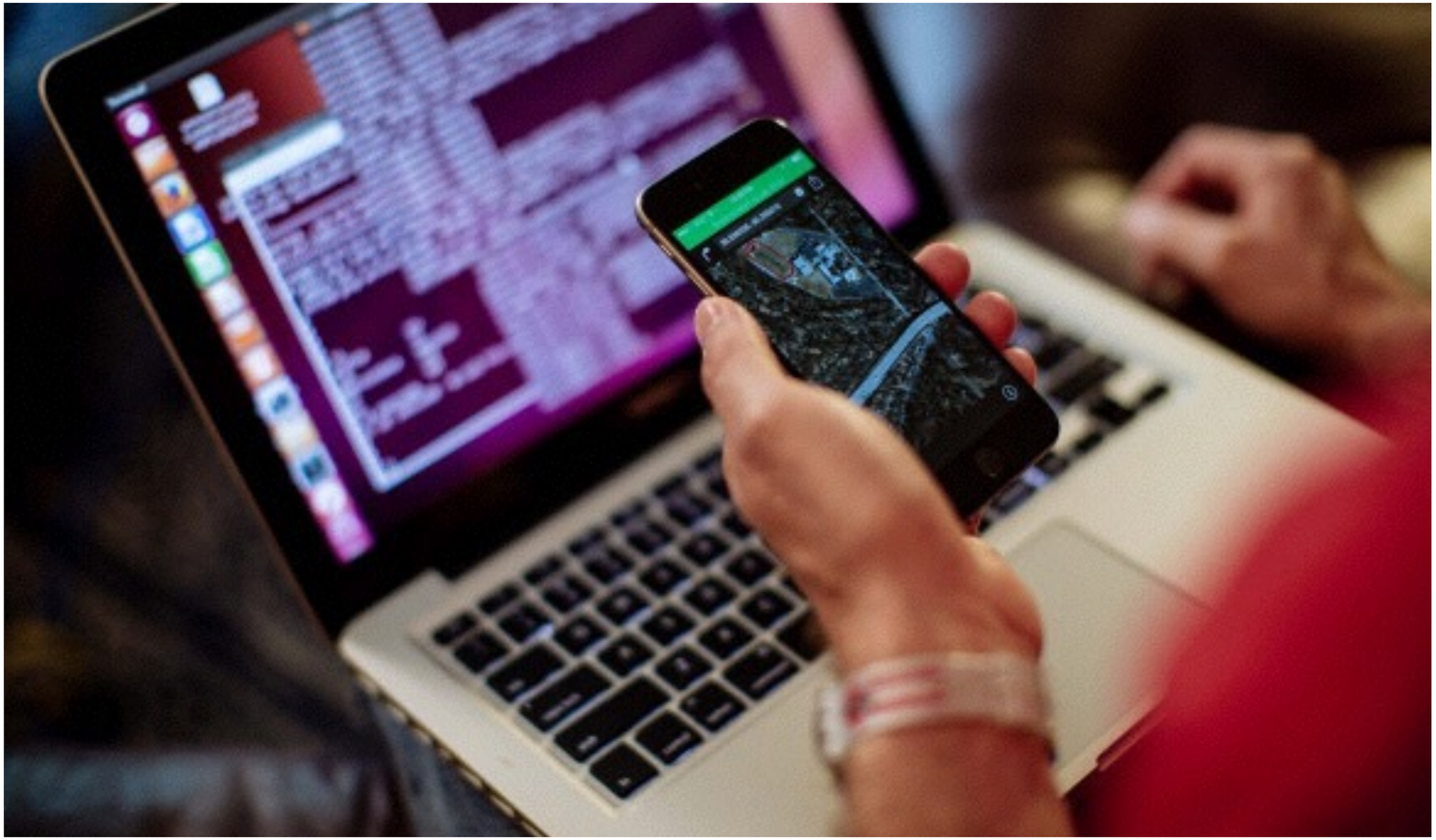
Left: Samsung SmartTV privacy policy, warning users not to discuss personal info in front of their TV
Right: 1984

10:35 AM - 8 Feb 2015

31,776 17,379

A febbraio 2015 si scopre che le condizioni di utilizzo di una **smart tv** Samsung sembrano uscite da un romanzo distopico di Orwell

Le smart tv vendute quest'anno saranno 27 milioni (Consumer Technology Association)

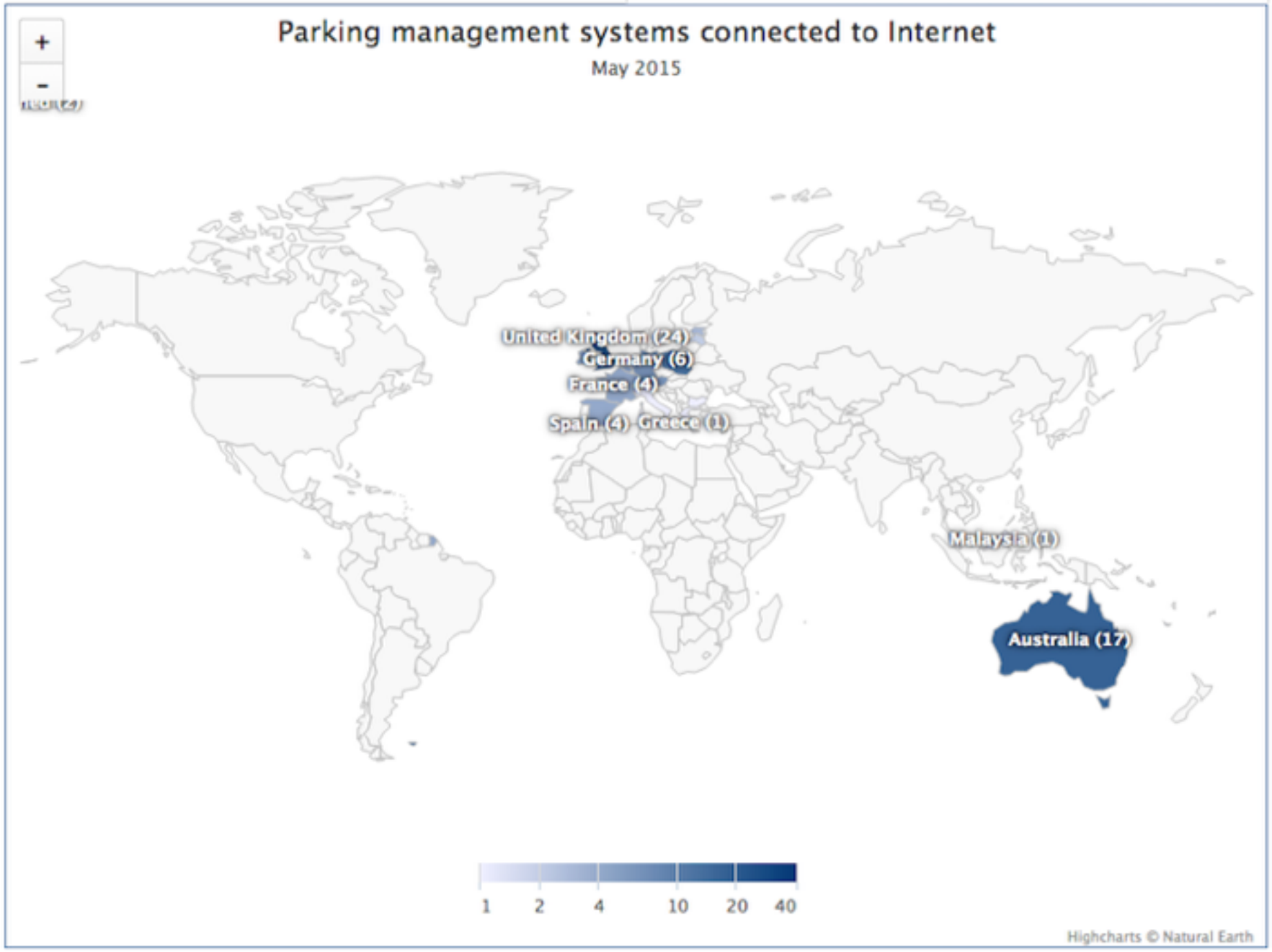


Estate 2015: due ricercatori riescono a **manipolare in remoto il motore, i freni, la trasmissione, l'impianto di condizionamento** di una Jeep Cherokee con a bordo il giornalista Andy Greenberg. L'hanno hackerata violando il sistema di entertainment connesso, Uconnect.

I veicoli vulnerabili, al momento della rivelazione, sono 471 mila. Fiat-Chrysler è costretta a inviare la patch via posta ai proprietari, in una scheda USB.


**Cartelloni pubblicitari spenti in remoto**, perché la API di una app Android per il controllo dell'illuminazione notturna - SmartLink - ha una serie di bug facilmente sfruttabili da hacker, dice il ricercatore indipendente Randy Westergren. Il sistema è usato da 60 mila cartelloni negli Stati Uniti. Westergren dice che è l'equivalente fisico di un ad blocker

"An attacker could exploit the vulnerability to shut off the lighting units for all of the billboards in the system"




Diversi **sistemi di gestione intelligente dei parcheggi** in garage sono hackerabili “da chiunque”, dice il ricercatore di Madrid, Jose Guasch, entrandone in totale possesso. I parcheggi hackerabili si trovano in tutto il mondo, dall’Australia alla Malesia, dalla Gran Bretagna a Francia e Germania.

L’hacker può facilmente ottenere le credenziali di accesso degli impiegati, controllando così la sbarra di ingresso e uscita, il sistema di pagamento - basta aggiungerci un malware, ed ecco rubati i dati delle carte di credito dei clienti - e perfino le videocamere di sicurezza.

Facile hackerare **sistemi di gestione del traffico** per creare ingorghi e caos nelle “smart city”: lo ha dimostrato già nel 2014 il ricercatore Cesar Cerrudo. È già successo a Los Angeles nel 2006. Ma era solo l’inizio: i progetti di “smart city” in corso sono 200, nel mondo.

“It’s a matter of time until someone launches an attack over some city infrastructure or system. Of course it’s not something simple, but it’s possible.”

# Rosso o verde, decide l’hacker

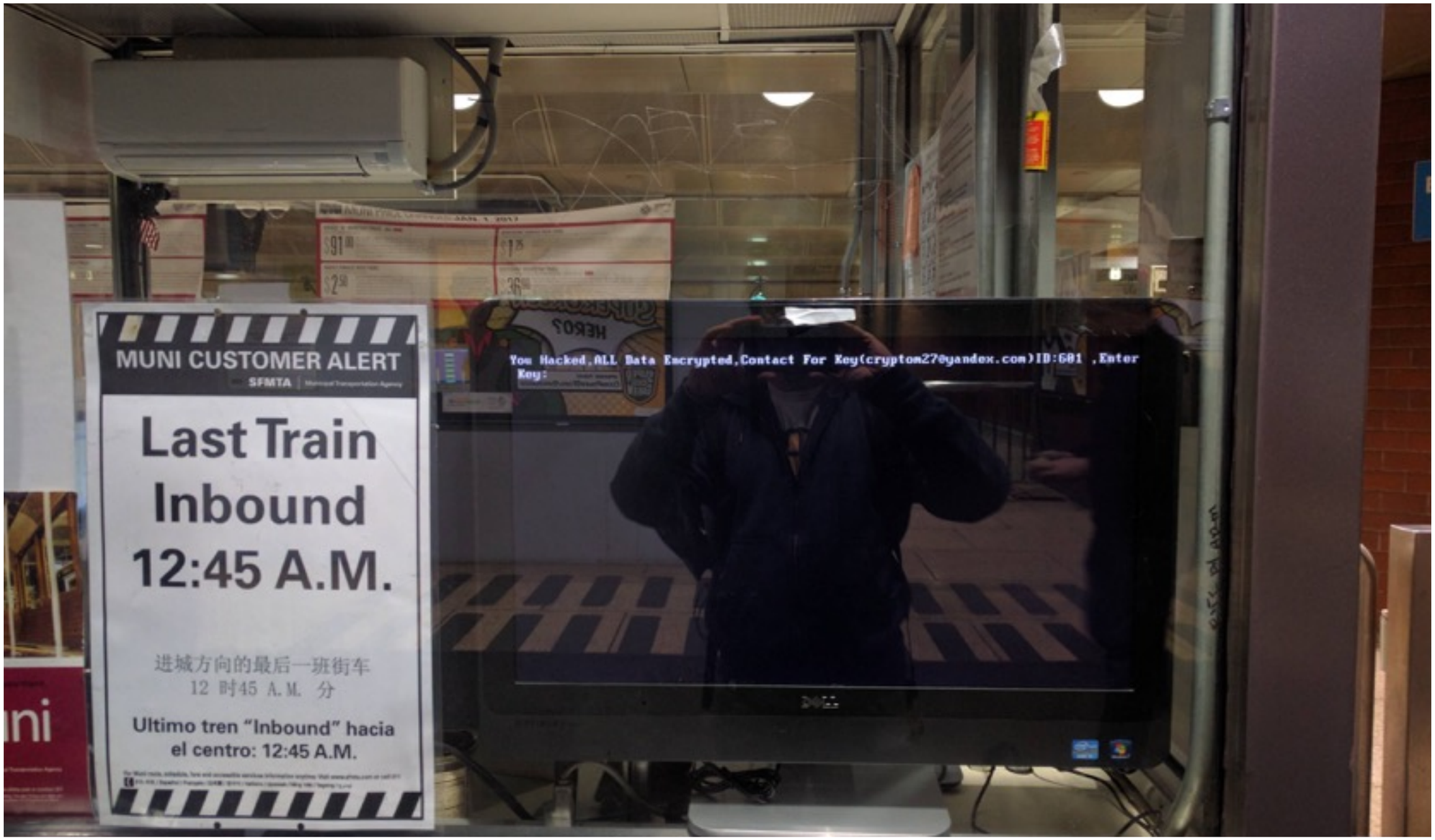
- Inchiesta di NBC sui **semafori intelligenti** di Econolite e Sensys Networks
- Bastano un laptop o un drone che voli sopra i semafori - i ricercatori ne hanno violati *mille,* perché senza password o cifratura di default
- “We could actually make the lights all red. We could change the light to be green in our direction”, dice Branden Ghena, dell’Università del Michigan
- Il rischio? “The real attacks here are where you clog up congestion in a city so you can turn all the lights to red and *people will be stuck in traffic jams for hours*”


Le **lampadine intelligenti Philips Hue** possono essere infettate da un virus informatico che costringe ogni lampadina connessa in wireless al sistema domestico a installare un update del firmware contenente un malware, che così diffonde il virus di lampadina in lampadina. Si può fare in remoto, fino a 400 metri di distanza.

Secondo il dottorando del Weizmann Institute of Science, Eyal Ronen, lo scenario peggiore è un black out di un'intera città dovuto ad hacking di un sistema di illuminazione intelligente, in cui le lampadine e i lampioni e le luci e i semafori si spengono tutti, di infezione in infezione.


**Pentole, macchine del caffè, lampadine e altri device domestici intelligenti** sono anche l'anello debole per violare dati contenuti su smartphone. Secondo due ricercatori, la app WeMo di Belkin per Android che li controlla - tra i 100 e i 500 mila download - aveva una vulnerabilità che consentiva ad hacker di violare i telefonini su cui quell'app era scaricata, e rubarvi così foto e tracciare i movimenti del proprietario.

Scott Tenaglia, di Invincea Labs: "The insecurity of my (Internet of Things device) now affects the security of another device I own, something that I probably care a lot more about than my IoT".




**Hacker entrano in possesso del sistema di trasporti pubblici "smart" di San Francisco, Muni**, il settimo più importante degli Stati Uniti, chiedendo un riscatto di 100 Bitcoin - circa 74 mila dollari - per rimetterlo in funzione. Se non viene pagato il riscatto, minaccia l'hacker, saranno rilasciati online database contenenti contratti e dati degli impiegati. Nel frattempo, decine di migliaia di passeggeri viaggiano gratis. Compromessi oltre 2000 computer, il sistema di pagamento, mail e per la geolocalizzazione in tempo reale dei bus.

Qualcosa di simile era già accaduto a Lodz nel 2008, quando un adolescente hacker aveva causato - trasformando un telecomando in una trasmittente a infrarossi - il deragliamento di quattro tram. Nello stesso anno era stato pubblicato un documento che mostrava come hackerare l'autorità che gestisce i trasporti pubblici nel Massachussetts.

# Caldo o freddo? Decide l'hacker

- **Termostati intelligenti violati**:
  - Caso dei device Nest che rivelano il codice postale degli utenti in chiaro, in rete
  - Ad agosto 2016, il *primo ransomware dedicato*: "One day, your thermostat will get hacked by some cybercriminal hundreds of miles away who will lock it with malware and demand a ransom to get it back to normal, leaving you **literally in the cold** until you pay up a few hundred dollars" (Lorenzo Franceschi-Bicchierai, Motherboard)


L'arcinoto hacker e troll 'Weev' costringe **14 mila stampanti connesse** a stampare volantini di propaganda neonazista

"I did not hack any printers, I sent them messages, because they were configured to receive messages from the public"



**Giocattoli "smart"**? No, un mercato da 2,8 miliardi in cui una Barbie diventa uno strumento di sorveglianza; un orsacchiotto rivela nome, sesso e data di nascita dei bambini che ci giocano; e un orologio dice agli hacker dove si trova sempre vostro figlio

“With **medical IoT**, hacking threats are scarier than just a night without Netflix and Twitter; they threaten the privacy of our medical information, or in extremely malicious cases, even lives”

**– Dov Greenbaum e Mark Gerstein, NyTimes**

# *IoT hell*, un paradiso per la sorveglianza

"In the future, intelligence services **might use** the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials"

- *James Clapper, direttore dell'intelligence USA*

# Che fare?

# Spediti verso l'inferno

- Molti produttori non si curano della sicurezza
- Molti clienti nemmeno
- Alcuni oggetti "smart" sono troppo *stupidi* per consentire di installare firewall
- Spesso le patch vanno applicate dall'utente, che non ne ha le competenze
- Gli attaccanti sono sempre più organizzati e competenti
- Il **70%** degli oggetti connessi è a rischio (HP, 2014)

# Oppure no?

- Il successo di “Mirai” e delle sue varianti sta nel successo di 62 username e password di default (“admin”, “password”, “123456”, “root”): sono sufficienti per infettare centinaia di migliaia di device
- Per evitarlo basterebbe **cambiare la password** con una più forte!
  - Lo dice il Computer Readiness Emergency Team del governo USA, lo dicono i produttori e gli esperti, lo dice il buonsenso

# Raccomandazioni concrete (del governo USA)

- Abilitare la sicurezza *by design*, di default
- Fare sì che le patch siano automatiche e per tutti
- Rivelare tempestivamente le vulnerabilità e come affrontarle
- Adottare la massima trasparenza sulla sicurezza dell'IoT
- *Connect carefully and deliberately*

# Raccomandazioni concrete (dei produttori)

- Usare la migliore crittografia disponibile
- Dotarsi di una *privacy policy* chiara e leggibile
- Sicurezza e privacy devono essere obiettivi dell'intera *supply chain* - dal produttore al rivenditore
- Il *support* deve essere garantito per tutta la vita del device IoT

"(…) the IoT will remain insecure unless **government steps in** and fixes the problem. When we have market failures, government is the only solution"

**– Bruce Schneier**

# *Bibliografia*


- http://blog.level3.com/security/attack-of-things/
- http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
- https://motherboard.vice.com/read/internet-of-things-mirai-malware-reached-almost-all-countries-on-earth
- https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html
- https://boingboing.net/2016/11/28/two-hackers-are-selling-ddos-a.html
- https://boingboing.net/2016/11/04/internet-of-things-botnet-thre.html
- https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
- https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
- https://motherboard.vice.com/read/a-flawed-android-app-for-billboards-made-real-life-ad-blocking-possible
- https://motherboard.vice.com/read/heres-a-map-of-hackable-smart-parking-garages
- https://motherboard.vice.com/read/all-the-ways-to-hack-a-smart-city
- http://www.nbcchicago.com/investigations/series/inside-the-new-hacking-threat/New-Hacking-Threat-Could-Impact-Traffic-Systems-282235431.html

- https://motherboard.vice.com/read/this-virus-automatically-kills-smart-light-bulbs
- https://motherboard.vice.com/read/how-hackers-could-steal-your-cellphone-pictures-from-your-iot-crock-pot
- http://www.slate.com/blogs/future_tense/2016/11/28/san_francisco_muni_hacked_for_a_ransom_payment.html?wpsrc=sh_all_mob_tw_bot
- https://motherboard.vice.com/read/nest-thermostat-leaked-home-locations-over-the-internet
- https://motherboard.vice.com/read/internet-of-things-ransomware-smart-thermostat
- https://motherboard.vice.com/read/hacker-weev-made-thousands-of-internet-connected-printers-spit-out-racist-flyers
- https://motherboard.vice.com/read/internet-connected-fisher-price-teddy-bear-left-kids-identities-exposed
- https://motherboard.vice.com/read/bugs-in-hello-barbie-could-have-let-hackers-spy-on-kids-chats
- https://motherboard.vice.com/read/a-gps-tracker-for-kids-had-a-bug-that-would-let-hackers-stalk-them
- http://www.nytimes.com/2016/11/03/opinion/a-cyberattack-and-medical-devices.html?_r=1
- https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper
- http://mashable.com/2014/08/02/internet-of-things-hacking-study/#xyNC34baGkqG
- https://www.us-cert.gov/ncas/alerts/TA16-288A
- https://motherboard.vice.com/read/we-need-to-save-the-internet-from-the-internet-of-things