&

Log In

POLICY FORUM Browse Topics Research Podcasts Resources Events Subscribe Contribute

Search

Are smart cities leaving us vulnerable to supervillains?

How to avoid ‘network error’ in a hyper-connected world

ANTHONY BERGIN, PAUL BARNES

PHOTO: ValeryBrozhinsky

Share in f 𝕏 g⁺ More

Republish

GOVERNMENT AND GOVERNANCE, INTERNATIONAL RELATIONS, NATIONAL SECURITY, SCIENCE AND TECHNOLOGY | AUSTRALIA, ASIA, EAST ASIA, SOUTH ASIA, SOUTHEAST ASIA, THE PACIFIC, THE WORLD

About the Author

11 SEPTEMBER 2018

The Internet of Things is being embedded into the world's cities at an

Bergin and Paul Barnes write.

Worldwide spending on technologies for smart city projects is estimated to reach $80 billion in 2018 and will grow to $135 billion by 2021.

But the smart cities revolution brings with it a raft of new security challenges facing cities, many of which are well set out in the recent findings from IBM's fascinating report, *The Dangers of Smart City Hacking.*

The report considers how Internet of Things (IoT) technology has resulted in hundreds of thousands of connected systems being embedded in many a city's critical infrastructures. The paper follows an investigation that discovered 17 zero-day (previously unknown) vulnerabilities in smart city sensors and controls used in cities around the world.

If left unpatched, they say, these vulnerabilities could allow a new breed of 'super villain' to access sensors and manipulate data to disastrous effect.

The researchers did penetration testing and practically demonstrated exploitable vulnerabilities, and, of course, informed device manufacturers and city users of the vulnerabilities to ensure they were patched ahead of referencing them.

The IBM report demonstrates creative thinking about how these vulnerabilities could be leveraged to cause real and significant disruptions to the systems they controlled. The exploits they found were also relatively basic – their existence is

Anthony Bergin

Dr Anthony Bergin is a senior research fellow at the ANU National Security College, and senior analyst at the Australian Strategic Policy Institute (ASPI).

Also by this Author

PNG border security a key strategic interest for Australia

ANTHONY BERGIN

Planning for the worst

ANTHONY BERGIN

See All

likely to be indicative of incomplete or inadequate design and integration practices.

technology to be hacked. It found that hackers could accomplish simultaneous traffic tie-ups on key city roads by taking control of traffic control infrastructure. Doing this would create traffic gridlock and delay police from accessing crime scenes.

Projected consequences considered both real and false disasters: by causing water level gauges, radiation detectors and other detection and alarm systems to “report incorrect data, an attacker could potentially cause an evacuation as a distraction”. A city could suffer far worse damage as a result of the delayed response to a radiation threat or other type of emergency.

There could even be agricultural crop manipulation. Farmers use sensors to measure humidity, rainfall, and temperature to efficiently irrigate crops and determine optimal harvest times. Manipulation of this sensor data could result in crop damage, targeting a specific farm or an entire region.

But how worried should we be?

In late 2016 the Ukrainian capital, Kiev, lost the equivalent of a fifth of its total power capacity for approximately an hour. While this might not sound like a far-reaching catastrophe, cybersecurity researchers determined that it may have been a dry run of malware designed to sabotage an electricity grid.

In January this year, a Hawaiian emergency management services worker sent a false alert warning of an incoming ballistic missile. The live alert was sent to radio

More on this:

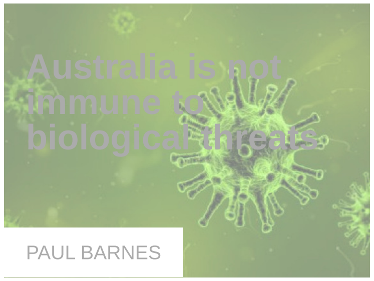
The artificial intelligence arms race

About the Author

Paul Barnes

Dr Paul Barnes is head of the Risk and Resilience Program at the Australian Strategic Policy Institute (ASPI).

Also by this Author



Australia is not immune to biological threats

PAUL BARNES

Are we ready? Healthcare preparedness . . . casualty events

PAUL BARNES

See All

and television stations, mobile phones of residents and visitors to the state.

The connectivity of the communications system created a

More on this:

Will smart cities become the next populist scapegoat?

Hawaii. Such a transmission could easily have been caused by a component failure or exploitation of a system's vulnerability.

The Hawaii incident underlines the surprise potential for the rapid spread of false alarms across our connected society.

The *New York Times* has reported evidence of attempts to hack the SCADA (computer-guided) controls of a small dam in New York State by individuals associated with Iran's Revolutionary Guards Corps, possibly attempting to trigger a damaging release of water. Some evidence linked this attempt to a wider plot to impact large US financial institutions targeting online access to bank accounts.

So what's the solution?

According to IBM, it's really a two-fold shared responsibility: the manufacturer's job to make sure that their products are designed and built with security as a key outcome, and the user's responsibility to make sure they are practising good security hygiene.

According to the IBM team, a series of steps by security administrators will go a long way to securing smart cities. These include implementing IP address restrictions for those who can connect to the smart city devices, especially if networks rely on the public internet; leveraging basic application scanning tools

You might also like

Getting ready to respond

PETER HUGHES

The risks of regional integration

IWAN J AZIS

Closing the country

ASHER HIRSCH

Australia's anxieties after the 'Age of Intervention'

JOANNE WALLIS

that can help identify vulnerabilities; using strong network security rules to prevent access to sensitive systems, as well as safer password practices; disabling unnecessary remote administration features and ports; taking advantage of

identify suspicious internet traffic; and hiring ethical hackers to test systems.

The steps really boil down to “do good basic security”. Unfortunately, the basics may not be as widely applied as needed, given the layered complexity of cyber systems both already in use and due to be rolled out.

We asked Melbourne’s Chief Resilience Officer Toby Kent what he thought of the findings of the *Dangers of Smart City Hacking* report. Toby acts as champion of Melbourne’s resilience efforts and coordinates policy efforts to develop holistic resilience strategies for the city.

“There is a certain irony as the interconnectivity of urban systems, which should add to the quality of life for many different city users, including in the avoidance and management of acute shocks, simultaneously make us more vulnerable.

“In Australia, our multiple tiers of government run the danger of too many in authority seeing the responsibility being someone else’s.

More on this:

China’s Big Brother smart cities

“In reality we need informed citizens acting sensibly, operating under effective national and state-led guidance. Victoria is the first State to launch a cyber-security strategy, run from the Department of Premier and Cabinet. This is an important step forward with many more to go, but too many local government

The challenge of Syrian refugees

JOHN HEWSON

Abe and Xi: a year to remember?

STEPHEN R NAGY

authorities remain exposed, both because of a lack of awareness of cyber risks and a lack of capacity to adequately address them.”

self-aware of personal online security behaviours, we must develop and sustain capabilities to design cybersecurity into our smart cities and related support systems.

This means being aware of legacy and modern cyber control systems and their exploitable vulnerabilities. In addition to removing existing vulnerabilities, where possible we need to promote resilient, secure design in our evolving city and urban landscapes.

In what seems to be an inexorable march toward a ‘ghost-in-the-machine’ future, the connectivity of our smart cities means maximising cyber safety isn’t just a ‘nice to have’ outcome. Waiting for a ‘network error’ makes no sense.

Back to Top

Share More Republish

Join the APP Society

Comments are closed.

Topics Arts, culture & society **Region** Australia **In Focus** Indo-Pacific **Legal** Terms and conditions

Belt and Road
Development
Economics and finance
Education
Environment & energy
Food & water
Government and governance
Health
International relations
Law
National security
Science and technology
Social policy
South China Sea
Trade and industry

Asia
East Asia
South Asia
Southeast Asia
The Pacific
The World

Poverty

Privacy
Comments policy

Partners
Crawford School of Public Policy
APPS
APP Society
ANU

Society
About The Society
Society Constitution
Join the Society

Australian National University CRAWFORD SCHOOL OF PUBLIC POLICY

ASIA & THE PACIFIC POLICY SOCIETY

Australian National University NATIONAL SECURITY COLLEGE