Expanding IoT poses cyber-security risks and intelligence collection opportunities

[Content preview – Subscribe to Jane’s Intelligence Review for full article]

The rapid expansion of the Internet of Things (IoT) is transforming the online ecosystem, with effects that have yet to be fully felt. Jane’s examines the way that governments around the world are responding to the essential tensions posed by the IoT, whose vulnerabilities make it both a national security threat and a data-rich environment for intelligence collection.

Key Points
• The expansion of the IoT presents data collection opportunities and entry points for intelligence agencies; however, for governments, these benefits are likely to be outweighed by the broader challenge of securing IoT devices against cyber attacks.
• Public attention has focused on the collection of audio or video data from IoT devices, but the greatest immediate security threat stems from the proliferation of relatively insecure networked devices in the online ecosystem.
• As the IoT expands, a ‘bow wave’ effect – with a future surge in the rate at which support is no longer available for older devices – could exacerbate the cyber-security challenges.

The Internet of Things (IoT) – in broad terms, non-core internet-linked devices of varying degrees of ‘smartness’ – has become an increasing focus for national cyber-security initiatives, even as its value for intelligence collection operations has become apparent. On 30 April 2019, the UK government convened a round-table meeting with IoT manufacturers to discuss IoT cyber-security issues, aiming to promote best practice and encourage further steps by manufacturers to secure their products. According to a UK government 21 May press release, “As increasing numbers of these devices are brought into our homes, it is now more important than ever for industry and government to address the issue.”

On 1 May, the UK also revealed draft legislation intended to improve the cyber security of IoT devices. Its provisions include a requirement for IoT devices to be sold with unique passwords and for manufacturers to advertise a public point of contact for the notification of vulnerabilities; it also creates a security labelling scheme and seeks manufacturer commitments to provide future security updates.

Speaking to Jane’s on 29 May, Dr Ian Levy, the technical director of the UK government’s National Cyber Security Centre, said, “It’s simply unacceptable that basic security problems
in consumer IoT devices continue to be discovered and reported vulnerabilities aren’t fixed.” Nonetheless, Levy noted, “Progress is being made on an innovative labelling scheme to improve consumers’ understanding about the devices they bring home.”

A rendering of the ‘smart city’ concept, drawing on the Internet of Things (IoT) and information communications technology. Poor security practices by users, technical limitations, and the ease of access may make IoT devices a primary target for cyber attackers in a smart city. (Metamorworks/Getty Images)

Although the UK has been a national pioneer in tackling the challenges of IoT security, the problem is globally recognised: on 25 January, for example, the Japanese government approved a legal amendment that permitted the country’s National Institute of Information and Communications Technology to attempt to break into Japanese citizens’ IoT devices using default passwords and password dictionaries, to assess security vulnerabilities. In October 2018, California passed a law – due to come into force in 2020 – banning default passwords in all new electronic devices and forcing a password change on first use.

However, as government initiatives to improve IoT security gather pace, there are two ‘flip sides’ to the necessary cyber defence of the IoT that have also received greater media and academic attention. First, the vast and exponentially increasing volume of data generated by IoT devices could be of use to signals intelligence (SIGINT) and human intelligence (HUMINT) agencies and law enforcement agencies, if IoT vulnerabilities can be exploited. Second, nation-states can exploit the IoT for cyber attacks and the delivery of covert action, either for conducting disruptive attacks on critical national infrastructure where connectivity is an issue or harnessing multiple connected devices to cause material damage.
This inherent tension in the IoT – cyber security versus intelligence collection – is also becoming more acute at a time when agencies are seeking to compensate for reduced access to the content of communications because of the increasing adoption of end-to-end encryption (E2EE). Jane’s has previously documented how – after the 2013 surveillance revelations by former US National Security Agency (NSA) contractor Edward Snowden – many threat actors migrated to platforms with E2EE, prompting agencies to look to other techniques and potential data sources.

In terms of techniques, a common approach with a low entry bar – readily accessible to agencies outside the ‘top tier’ – is equipment interference (EI), which essentially covers hacking devices themselves. The collection of communications metadata, which is often not encrypted, is another, separate technique. EI and metadata exploitation pre-date ubiquitous encryption and have sat alongside access to content by passive interception for many years.

Government agencies’ loss of access to much digital content because of E2EE is unlikely to be reversed. However, the acceleration of the digital revolution also affords data-rich opportunities in the rapid proliferation of sensor-based technology and the increasingly hyperconnected nature of sources. The scale of adoption of the IoT suggests more opportunities for SIGINT agencies using EI and interception.

**Defining the IoT**

IHS Markit describes the IoT not as a market or a set of devices, but as a movement – a trend towards the inclusion of networked technology and sensors into physical devices that would not previously have been connected to the internet. IHS Markit estimated that there were 27 billion connected IoT devices worldwide in 2017, with this number increasing to 31 billion in 2018 and projected to reach 125 billion by 2030. The pending shift to 5G network technologies will almost certainly contribute to the expansion of the IoT, enabling more devices to exchange larger quantities of data.

The implications of the expansion of the IoT in some respects parallel the uptake in smartphones and other connected personal devices. However, these are comparatively high-end pieces of technology that are designed from the ground up to be connected and are manufactured by a comparatively small number of major companies. They also generally adhere to well-established standards for communications and security.

[Continued in full version...]

(795 of 4200 words)
For the full version and more content:

Jane's Military & Security Assessments Intelligence Centre

This analysis is taken from Jane's Military & Security Assessments Intelligence Centre, which delivers comprehensive and reliable country risk and military capabilities information, analysis and daily insight.

IHS country risk and military capabilities news and analysis is also available within Jane's Intelligence Review. To learn more and to subscribe to Jane's Intelligence Review online, offline or print visit: http://magazines.ihs.com/

For advertising solutions visit Jane's Advertising