RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 105 – 27 May 2019

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced with prior permission from RSIS and due recognition to the author(s) and RSIS. Please email to Mr Yang Razali Kassim, Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

Defending Forward: Pre-emption in the Internet of Things

By Phillip Lohaus

SYNOPSIS

America's recent shift from "active defence" to "defending forward" in cyberspace has left some observers nervous. As the attack surface of the Internet rapidly expands, however, a strategy focused solely on defence will do little to incentivise adherence to international security norms. China is particularly vulnerable in the space known as the "Internet of Things," creating an opportunity to balance the use of carrots with sharper sticks.

COMMENTARY

THE UNITED STATES recently shifted its cyber security approach from "active defence" to "defending forward." This seemingly small difference in semantics nonetheless signals a departure from prior cyber security doctrine.

Whereas the previous strategy relied primarily upon defensive measures and the construction of international norms, "defending forward" implies a more engaged and perhaps offensive stance of mitigating threats through pre-emption. When combined with private sector partnerships and enhanced standards and regulations, this strategy shift will allow the US to deter potential cyber security adversaries as the Internet rapidly expands, including those in East Asia.

More Things, More Problems

The timing of this policy change is propitious as the attack surface is rapidly expanding. Since 2015, the number of devices connected to the Internet has increased by nearly 40 percent. The vast majority of this growth is attributable to devices that autonomously communicate with one another, often via unsecure protocols.

The sheer variety of these devices and the methods by which they communicate has thus far stymied the development of universal security standards. Yet these devices, collectively known as the "Internet of Things" (IoT), will make up the majority of Internet-connected devices after 2021.

The US government is only beginning to understand and mitigate its IoT security risks. Whether in national energy and health infrastructure or American military hardware, expanded connectivity has increased the number of potential targets and pathways available to cyber attackers. In a 2018 report, the Government Accountability Office found that weak passwords, unencrypted communications, and unpatched bugs have turned the "fundamental enablers of the Defense Department's modern military capabilities" into security liabilities.

It is a little surprise that the Director of the Defense Intelligence Agency singled out IoT as one of the most "important emerging cyberthreats to national security" that same year.

Security & Public-Private Partnerships

Public-private partnerships are critical to enhancing IoT security. While industry often operates critical infrastructure and produces security technology, government makes policies and regulations for critical infrastructure and is a consumer of commercial technology solutions. As industries fold IoT devices into their supply chains and daily operations, they too are increasing the number of exploitable pathways for would-be cyber attackers.

Infected IoT devices can be aggregated into massive botnets to launch Distributed Denial of Service (DDoS) attacks, or to send automated spam messages. Ransomware can degrade the operation of IoT devices leading to the disruption or manipulation of CCTV recordings. Security concerns, in fact, top of the list of factors inhibiting an even wider adoption of IoT technology, according to global consulting firms McKinsey and Bain.

Standards and regulations are important components of enhancing cyber security, but they do little to change the global dynamics that drive hacking and cyber-attacks. Recently-proposed legislation in the US Congress aims to create common security standards for IoT devices, but its scope is naturally limited to American companies or those that contract with the US government.

California's IoT law, passed in September 2018, requires IoT device manufacturers to address specific vulnerabilities such as default passwords. But industry regulations cannot be viewed as panacea either as they risk stifling innovation and similarly have limited jurisdiction. Each of these initiatives aims to create better security defences in the IoT space.

But communicating clear consequences for bad behaviour globally will require the selective demonstration of active defence cyber capabilities. A bill allowing companies to engage in such behaviour was introduced to Congress in 2017, but was never passed into law.

Crisis Comes with Opportunity

Though the wisdom of allowing the private sector to engage in active cyber defence remains the subject of debate, the US government is beginning to demonstrate its willingness to "hack back," particularly with respect to China. In March, the Washington Times reported that the US had begun counter-attacks on China in response to ongoing cybertheft.

Some prominent cybersecurity commentators have suggested that this shift in approach will lead to a "dangerous escalation of cyber conflicts" or that it will undermine relations between the US and named countries. Because the change in American strategy occurred after China engaged in cyber intrusions and espionage against the US, however, it is more of a response to bad behaviour than an unprovoked escalation.

China's pattern of behaviour in cyberspace provides a clear indicator of how it might behave in the expanded attack surface created by IoT. According to documents published by Chinese officials, China aims to both become a leader in a number of emerging technologies and to maintain its "first mover ability" in a number of spaces relevant to IoT. Good defences will lower the success rate of cyber-attacks and mitigate their fallout, but will do little to incentivise China to change its strategies or behaviors.

Just as China has exploited weaknesses in the cyber defences of America, its allies, and the private sector, the US and allied governments should also consider the weaknesses in China's cyber defences, particularly in the IoT space. A recent study exposed a security flaw in the peer-to-peer communications of millions of IoT devices, from security cameras to baby monitors; 39 percent of these devices were located in China, and only seven percent are in the US.

In a 2017 report on Chinese IoT security, NSFOCUS found thousands of Chinese router exposures, and video monitoring giants Dahua and Hikvision were found to have nearly one million exposed devices operating in China. The IoT space thus provides a target-rich environment in which others may selectively "defend forward" and impose costs in the event of future Chinese cyber-attacks and intrusions.

Carrots are Tastier when Sticks are Sharper

Authoritarian governance, as employed in China and the other countries named in the 2018 Cyber Security Strategy, facilitates a "whole of nation" approach to cybersecurity. For democracies, public-private partnerships, standards, and regulations are critical to leveling the security playing field, but deterring future attacks will require the extra step of selective and proportional cost imposition.

As the Internet expands rapidly to incorporate IoT devices, "defending forward" will allow the US to mould behavioural expectations and impose costs from multiple angles. To retain the first-mover advantage, the US must defend forward not just at the Internet edge, but also alongside it.

Phillip Lohaus is a Visiting Fellow in Foreign and Defence Policy at the American Enterprise Institute, where he focuses on emerging security threats and competitive strategies. He contributed this to RSIS Commentary.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg