INTERNET OF THINGS & THE CYBER THREATS TO DIGITALISATION: A NATIONAL SECURITY REVIEW

RAMNATH REGHUNADHAN

School of International Relations & Politics
Mahatma Gandhi University, Kottayam

The phrase "Internet of Things" (IoT) as a conceptual paradigm was introduced by consumer sensor expert and innovator Kevin Ashton during a presentation to the company Procter and Gamble (P&G) in 1999. (Marr, 2015) He believes that unlike the twentieth century computers that "were brains without senses," in the twenty-first century, and can "sense things for themselves." (Gabbai, 2015) The European Union Agency for Network and Information Security (ENISA) describes IoT as an "ecosystem where interconnected devices and services collect, exchange and process data... to adapt dynamically to a context... [and] is [linked]... to cyber-physical systems...[enables]... Smart Infrastructures by enhancing their quality of service provisioning." (ENISA, 2017) The IoT is an emerging paradigm having inherent technical, socio-economic aspects that are of greater significance. It is considered to be a concept that is still evolving and is being understood and/ or perceived as well. It comprises of a wide range of factors in an ecosystem of interconnected and interrelated devices as well as services; in the likes of sensors, smart consumer goods, and even components of industry and health sector. These emerging technologies will be able to gather, exchange, trade and/ or even process any quantity of data in enabling adaptation to any particular context; is even capable to transform businesses and even the way we live as a whole. It is closely connected to cyber-physical systems, with respect to emerging and potential (future) safety implications. According to Narang Kishor of Narnix Technolabs, "The IoT... is... about connecting everything that exists with everything else... [It] is a neural network of globally aware, intelligent and heterogeneous devices connected with each other in multiple ways..." (Teamefy, 2017)

The glocal (global-cum-local) nature of the incidences have but created greater issue in effectively dealing with them; technologically as well as legally. The increasing concern have but emerged due to issues of "data breach" as well as "hacking" that is but emerging as a concern. (Teamefy, 2017) The emergence of "smart cars as systems providing connected, added-value features in order to enhance car users experience or improve car safety... encompasses use [of] telematics, connected infotainment or intra-vehicular communication." (ENISA, 2016) Wismonskey of the Cyber Security Research Center at the Hebrew University of Jerusalem argues opined that the smart cars usually contain "software, communication devices, and computer-based hardware than ever before, often connected to a wired and even wireless network. These vehicles are based on the CAN Bus (Controller Area Network) - a network that connects the electronic components of the vehicle and is largely responsible for its operation; from the use of electric windows to the use of vehicle brakes." Thus in case of a targeted attack on a smart car, it would but threaten the safety and privacy of passengers as well as other citizens. These can increase incidences of "remote attacks, persistent vehicle alteration, theft and surveillance." (ENISA, 2016)

In 2015, Charlie Miller (a Security Researcher at Twitter), and Chris Valasek (the Director of Vehicle Security Research at IOActive) exposed the vulnerability from remote attacks by taking control of a Jeep using zero-day exploits, which forced the recalling of around 14 lakh vehicles. (Greenberg, 2015) Hackers (both whitehat and blackhat), as well as various governments, have identified vulnerabilities in regard to cars of companies like Tesla, Volkswagen, BMW causing greater socio-economic and political repercussions in different nations. (Kumar, 2016, Khandelwal, 2016) Now airports can be considered as gateways to almost any country or city that intend to create a better impression for visitors, tourists and even for enabling a viable business investment. Unlike the conventional functionality to enable transit from one place to another, the 21st century is seeing the evolution of airports to smart airports. The smart airports can be defined as "those airports making use of networked, [data-driven] response capabilities... implementing new smart components to offer... a portfolio of services... from self or automatic check-in, baggage & document check, flight booking management and way finding services to automated border control and security checks." (ENISA, 2016) This includes smart airport solutions including "smart gates, beacon technology, mobile devices to navigate the airports and face recognition systems, to air traffic management, baggage and check in management, IP-based security monitoring, communications, ticketing, and information systems, freight operations information

systems, air traffic management and airways analytics." (NATS Limited, 2018) This interconnectedness of various components and/ or devices can also create possibilities for much advanced but multitude of attacks that could "expose airport assets to a larger attack surface." (ENISA, 2016) An estimated number of global passengers being expected to increase to seven billion within the next two decades, airports will have to ensure they are able to deal with these humongous traffic and demand. A recent study on the market potential of smart airports has been estimated to be around 13.5 billion USD within two years. (NATS Limited, 2018) But this increases the possibilities of potential vulnerabilities, particularly when the security measures in place are lacking. There are instances like in July 2016 hackers (allegedly Chinese) successfully infected two largest airports in Vietnam as well as the national airlines, the European multinational company Airbus is reportedly hit by a dozen big cyber attacks each year (Coyne, 2016; ENISA, 2016) and so was airports in Thiruvananthapuram (2016) as well as in Perth (2017). (Indian Express, 2016; Butterfly, 2017)

The emergence of Smart Cities with the objective to optimize the city in a dynamically new way could enable a better quality of life to the population, particularly by the application of Information and Communication Technologies (ICTs). This will see the evolution of interconnected cities, where data exchange will be prevalent at a larger scale. The "Intelligent Public Transport (IPT) systems" will be a key component of the Smart Cities, and will manage the local public transportation

lost money to hackers, who used the information on their identity and credit cards to conduct theft. (Strickland, 2016) In 2015, the attack from ransomware CrptoWall was estimated to have cost victims 18 million USD in damages. In 2016, a hospital in Los Angeles was held for ransom, where hackers demanding 3.7 million USD to be paid in Bitcoin to get the decrypting tool. (Balakrishnan, 2016)

In the Digital India, there will be interconnected devices and services that collect, exchange and process data in order to adapt dynamically to the emerging challenges of governance and sustainability. It has come even come to our homes, viz.a.viz. Smart Homes, where devices are interconnected and integrated to the "Home Area Network," to be connected at real-time with the end-user/owner in order to provide for greater quality of life for citizens. Consequentially this can have a negative impact on the life, health as well as the safety of individuals as well. (ENISA, 2015) There emerges issues like loss of privacy, greater vulnerability to attacks by actors unknown, with greater ramifications to the user. There is an

increased possibility of victimisation of the citizen-user, which will have greater impact on the socio-economic and psychological aspects of the person. There also exists challenges and ensuing security issues in various IoT goods, products as well as services that compromises the security measures in place. There are greater concerns on the emerging complexity of problem related to cybercrimes that can subsequently jeopardise a person's safety, security and more importantly privacy. IoT extraordinarily transforms the manner in which personal data is being collected, analysed, used, and most importantly protected. There are pertinent issues related to the adoption of IoT, besides the technical-cum-security issues and interoperability problems, the legislative and regulatory hindrances, challenges and/or bottlenecks that often exacerbate the existent problems and issues. The technological revolutions that take place coupled with the possibilities of IoT could actually outpace the capability of the related legislative and regulatory structures in adapting, particularly in an environment where clearly demarcated security guidelines and framework is lacking.

REFERENCES

1. Balakrishnan, Anita. (2016): The hospital held hostage by hackers, available at <https://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html>
2. Butterfly, Nick. (2017): 'Significant amount' of sensitive security data stolen in Perth Airport hacking, available at <https://thewest.com.au/news/wa/significant-amount-of-sensitive-security-data-stolen-in-perth-airport-hacking-ng-b88686393z>
3. Coyne, Allie. (2016): How Airbus defends against 12 big cyber attacks each year, available at <https://www.itnews.com.au/news/how-airbus-defends-against-12-big-cyber-attacks-each-year-418131>
4. European Union Agency for Network and Information Security (ENISA). (2015): Cyber security and resilience for Smart Hospitals, available at <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals>
5. European Union Agency for Network and Information Security (ENISA). (2015): Cyber Security and Resilience of Intelligent Public Transport Good practices and recommendations, available at <https://www.enisa.europa.eu/publications/good-practices-recommendations>
6. European Union Agency for Network and Information Security (ENISA). (2015): Security and Resilience of Smart Home Environments, available at <https://www.enisa.europa.eu/publications/security-resilience-good-practices>
7. European Union Agency for Network and Information Security (ENISA). (2016): sector in Smart Cities, available at <https://www.enisa.europa.eu/publications/smart-cities-architecture-model>
8. European Union Agency for Network and Information Security (ENISA). (2016): Cyber Security and Resilience of smart cars Good practices and recommendations, available at <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>
9. European Union Agency for Network and Information Security (ENISA). (2016): Securing Smart Airports, available at <https://www.enisa.europa.eu/publications/securing-smart-airports>
10. European Union Agency for Network and Information Security (ENISA). (2017): Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, available at <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>
11. Gabbai, Arik. (2015). Kevin Ashton Describes "the Internet of Things, available at <https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/>
12. Greenberg, Andy. (2015). Hackers Remotely Kill a Jeep on the Highway - With Me in It, available at <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
13. INDIAN EXPRESS(2016): Thiruvananthapuram airport's website, which was hacked, restored now, available at <http://indianexpress.com/article/india/thiruvananthapuram-airports-website-hacked->

-pakistani-group-claims-responsibility-4448188/

14. Khandelwal, Swati. (2016): Flaw Allows Attackers to Remotely Tamper with BMW's In-Car Infotainment System , available at <https://thehackernews.com/2016/07/bmw-hacking-smart-car.html>

15. Kumar, Mohit. (2016): Researchers Show How to Steal Tesla Car by Hacking into Owner's Smartphone <https://thehackernews.com/2016/11/hacking-tesla-car.html>

16. Marr, Bernard. (2015): A brief history of big data everyone should read, available at <https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/>

17. NATS Limited. (2018): Transforming the Airport Experience: The Future of Smart Airports, available at <https://www.nats.aero/apac/august-enewsletter/transforming-airport-experience-future-smart-airports/>

18. Strickland, Eliza. (2016): 5 Major Hospital Hacks: Horror Stories from the Cybersecurity Frontlines, available at <https://spectrum.ieee.org/the-human-os/biomedical/devices/5-major-hospital-hacks-horror-stories-from-the-cyber-security-frontlines>

19. TeamEfy. (2017): Security in IoT, available at <https://smart.electronicsforu.com/2017/11/03/3087/>

20. Techdirt. (2017): 'Smart' Hospital IV Pump Vulnerable To Remote Hack Attack, available at [https://www.techdirt.com/articles/20170920/09450338247/smart-hospital-iv-pump-](https://www.techdirt.com/articles/20170920/09450338247/smart-hospital-iv-pump-vulnerable-to-remote-hack-attack.shtml)

[-vulnerable-to-remote-hack-attack.shtml](https://www.techdirt.com/articles/20170920/09450338247/smart-hospital-iv-pump-vulnerable-to-remote-hack-attack.shtml)

21. Tracy, Philip. (2016): Cities are getting smarter-and much easier to hack, available at <https://www.dailydot.com/debug/smart-city-hack-cybersecurity-prevention/>

22. Young, Christopher. (2015): Why hackers want your health-care data, available at <https://www.cnbc.com/2015/05/27/why-hackers-want-your-health-care-data-commentary.html>