IoT Technological Development: Prospect and Implication for Cyberstability

Syarulnaziah Anawar[1], Nurul Azma Zakaria[2], Mohd Zaki Masu'd[3], Zulkiflee Muslim[4], Norharyati Harum[5], Rabiah Ahmad[6]
Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka,
Melaka, Malaysia

***Abstract*—Failure to address the risk poses by future technological development could cause devastating damage to public trust in the technologies. Therefore, ascendant technologies such as artificial intelligence are the key components to provide solutions for new cybersecurity threats and strengthen the capabilities of the future technological developments. In effect, ability of the technologies to prevent and withstand a cyber-attack could become the new deterrence. This paper will provide gaps to guide the government, industry, and the research community in pursuing Internet of Things (IoT) technological development that may be in need of improvement. The contribution of this paper is as follows: First, a roadmap that outline security requirements and concerns of future technology and the significant of IoT technology in addressing the concerns. Second, an assessment that illustrates the expected and unexpected impact of future technology adoption and its significant geopolitical implication on potential impacted areas such as regulatory, legal, political, military, and intelligence.**

***Keywords*—Internet of things; cybersecurity; geopolitical; artificial intelligence; technology adoption**

I. Introduction

The proliferation of smart devices in this era has opened an abundance of new opportunities for future technology growth in order to improve quality of life. The ongoing technological advance has turned the Internet of Things (IoT) devices into a necessity; Gartner [1] estimates that the number of devices that will be connected to the Internet is set to reach 20 billion by 2020. However, the security risk will increase in line with IoT growth, where the devices may not include advanced cyber security features due to processing power and operating system limitations. The risk is further deepened with the vulnerabilities and undetected threats of IoT technology that may prove devastating to cyber stability. This briefing paper presents a summary of assessment relative significant solutions in mitigating IoT security concerns, and facilitates the exploration and improves understanding of the potential impacts of recent advancements in the IoT as it pertains to cyber stability.

The proposed study is a multidisciplinary study devoted to landscape the prospects of future technological developments in many domains. The aim of this study is to present the current evidence and critical assessment relative to the potential and implications of future technological developments on international security as it pertains to cyber stability. The objectives of this paper is three-fold: First, to design a roadmap that outlines security requirements and concerns of future technology and the significant of IoT technology in addressing the concerns. Second, to assess expected and unexpected impact of future technology adoption and its significant geopolitical implication on potential impacted areas. Third, to provide recommendations for geopolitical risk mitigation.

The rest of this paper is organized as follows: Section 2 provide an overview of IoT Technology and the IoT security concerns. In Section 3, the basic concepts of potential ascending technology in addressing IoT security requirements and concerns is outlined, and the roadmap for IoT security mitigation is presented. In Section 4, provides foresight and in-depth analysis, which facilitate the exploration and improve understanding of the potential impact of recent advancements in the Internet of Things (IoT). Finally, we present the significance of the geo-political effect of future technology adoption and the strategic considerations for geopolitical risk mitigation in Section 5 and Section 6. This paper is concluded in the last section.

II. IoT: Technology Overview and Security Concerns

A. IoT Platform Framework for Public Internet

IoT is an interconnected network of physical objects embedded with sensors and can communicate over the Internet. The IoT platform framework utilized in the present study is shown in Fig. 1. The proposed framework is derived from TCP/IP model, consisting of IoT technology layers and components [2][3]. The IoT platform framework is classified into four technology layers: smart device/sensor layer, network/communication layer, service and application support layer, and application layer, while the IoT component is categorized into infrastructure and protocol.

Various protocols and technologies have been standardized and are widely used in IoT application. The standards have been deployed independently based on layers [4] without considering interoperability among consumers, businesses and industries. The interoperability standard is crucial for IoT application, to ensure data connectivity and data sharing from all IoT devices, managed by different parties, without neglecting security matters.

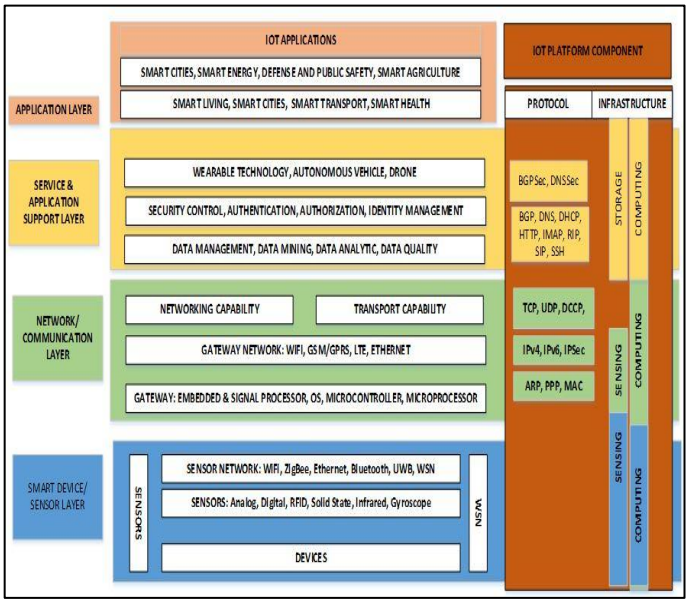

Fig. 1. IoT Plat form Network (Adapted from [2][3]).

B. IoT Security Challenges and Solutions

The increasing usage of the IoT has led to most IoT users facing a number of security challenges. The list of IoT implementation challenges and solutions is as follows [5]-[8]:

1) Authentication and authorization: The IoT is utilizing the Internet to connect users globally. For IoT data transmission, the challenge is to secure end-to-end communication between IoT devices. Authentication credentials can be easily tampered if data transmissions are inadequately encrypted or integrity of the communications are not verified. Currently, Internet Protocol Security (IPSec) and Datagram Transport Layer Security (DTSL) are the applicable solutions, which offer channel security services to overcome the authentication and authorization flaws in existing IoT protocols. IPSec, an authentication mechanism, is a set of protocols which offer a channel security service to the Internet protocol and has the advantage of protecting all higher layer protocols.

2) Data privacy: The data collected by IoT devices like geolocation, biometric and user behaviour information is sensitive and personal. IoT consumers are vulnerable to data breaches and unlawful surveillance especially when the data is transmitted to the IoT cloud platform. The current solution available is the General Data Protection Regulation (GDPR). This regulation proposes the usage of pseudonymization combined with encryption to offer a layer of data privacy protection.

3) Interoperability: IoT applications are penetrating the Internet across different service providers. The communication between service providers can cause security issues such as masquerading or route poisoning. The current solution for such interoperability issues among service providers is to implement Border Gateway Protocol Security (BGPSec). BGPSec is utilized to minimize the inter-domain routing weaknesses because it imposes the cryptography concept, safeguarding the route information sharing. BGPSec consists of two features, Autonomous System (AS) authorization and AS-Path footprint validation [9], which curb issues relating to route hijacking.

4) Malware threats: In IoT ecosystem, wherein all devices are connected to the Internet, malware attacks are prone to happen. With the limitation of resources in IoT devices, lightweight Intrusion Detection System (IDS) is a feasible option to ease the malware penetration issue. IoT devices work as an agent where the traffic will be analysed remotely at a centralized control panel. Lightweight IDS will reduce the energy consumption and should fit in with the limited IoT device capabilities.

5) Firmware vulnerability: An IoT device faces a challenge in terms of firmware vulnerability because of the presence of a 'backdoor' in its firmware. Thus, the system administrator should study ways in which to overcome the vulnerability issues. Firmware updates require the IoT devices to interact with the domain servers. However, these firmware update activities may lead to a DNS cache poisoning attack. Thus, implementation of the Domain Name System Security (DNSSec) ensures the IoT devices only receive authentic firmware updates. DNSSec acts as a security mechanism to avoid Internet users being redirected to fraudulent websites [10]. Moreover, DNSSec is designed to guard Internet users from receiving unlawful DNS data.

6) IoT device capabilities: The IoT devices may not include advanced cyber security features due to processing power and operating system limitations. Small devices like optical sensors and health wristbands with limited wireless signals and low resilience dominate IoT sensors. Hence, the potential security solutions such as anti-virus will cause high energy consumption which results in the IoT device's failure due to the amount of power being drained.

In short, various efforts have been made to overcome security issues in IoT implementation but the current solutions still have weaknesses that need to be addressed as summarized in Table 1.

TABLE I. SECURITY CHALLENGES VS CURRENT SOLUTION

IoT Architecture Layer	**Security Challenged**	**Current Solution**
Application Layer	Authentication and Authorization	IPSec, DTLS
	Data Privacy	GDPR
Service and Application Support Layer	Interoperability	BGPSec
Network Layer	Malware Threats	Lightweight IDS
	Firmware Vulnerability	DNSSec
Device Layer	IoT Device Capabilities	lightweight security solutions

III. Towards a Secure IoT: Implications of Ascendant Technology

A. Potential of Ascendant Technology

Ascendant technology is a technology with advanced capability to influence the progression of the IoT platform and is able to provide solutions for the IoT platform. Currently, ascendant technologies include artificial intelligence, deep learning, blockchain and quantum encryption.

Artificial Intelligent (AI), machine learning and deep learning are interconnected. AI refers to the involvement of a machine that is able to perform task similar to the characteristic of human intelligence [11]. Sequentially, AI includes planning, understanding input, identifying objects and sounds, learning, and problem solving, all activities that do not involve humans. Machine learning is used to attain artificial intelligence in which the machines have the ability to perform a task by training themselves to make a prediction about something using algorithms on a large amount of data. One of the ascendant techniques of machine learning is deep learning. Deep learning replicates the human brain structure, which consists of several discrete layers of neurons that are connected to each other and each layer has the function to learn a specific content before finally producing a decision.

Blockchain technology is another emerging, powerful technology that links with the cryptography element and contributes towards the IoT solution. The set of blocks is disseminated over a peer-to-peer network [12]. Blockchain refers to a distributed ledger that utilizes encryption to store perpetual and tamper-proof records of transaction data which are validated through peer consensus. Blockchain is used widely in cryptocurrency realms and consists of genuine data and it is operated not by any single person but by peer technology adoption. It is able to provide secure transactions and remove any centralization control, which might impact significantly on aspects of mobile payments, property ownership records and smart contracts in the future.

Cryptography and Quantum cryptography are the main cores of blockchain technology. Quantum Cryptography applies the science of exploiting quantum mechanics properties in encrypting and decrypting data [13]. Encryption of data is generated and communicated to the receiver utilizing photon light, which has a unique property. If the photon light is captured before the receiver's arrival, the photon properties will alter, consequently changing the key and making it unusable. Once photon light is produced, any kind of tampering will alter its property, hence, making it fit to be utilized in a cryptographic system, which in turn protects the key. This technology is beneficial as all sensor devices are linked remotely from the centralized processing center; hence, emphasizing the need to secure key exchange in data encryption.

B. The Roadmap: Mitigating the Security Concerns in the IoT

Currently, ascendant technology is utilized to boost decision-making, recreate business models and ecosystems, and reform customer experience. Fig. 2 shows where these technologies can be used in overcoming the security challenges of the IoT platform.

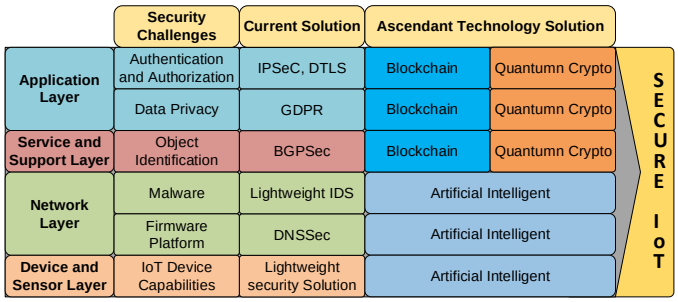

Fig. 2. Ascendant Technology and IoT Security Challenges.

C. Ascendant Technology: Risk and Benefit Analysis

Table 2 shows the risks and benefits of related ascendant technology in handling these security challenges.

TABLE II. Risks and Benefits of Related Ascendant Technology

IoT Layer	Security Challenge	Proposed Solution	Benefits	Risks
Application	Authentication and Authorization	Blockchain can be used to keep information of users and devices in the blockchain ledger. Every end-to-end communication will be authenticated by referring to the blockchain structure.	Tracking only authorize and authenticate sensor device connected to the IoT platform.	Computation and memory resources of the sensory device is limited yet the computation to use the blockchain and quantum crypto is high [14][15].
	Data Privacy	Data stored in blockchain can be control and accessible only by user [16].	Eliminating data privacy violation.	
Service and Application Support Layer	Interoperability	Blockchain and Quantum Crypto allow devices to add transactions to the ledger securely. Transactions are verified and confirmed by other participating devices in the network [17].	Establishing trust between IoT sensors device and main processing center without 3rd party.	

Network Layer	Malware Threats	Anomaly detection with AI technologies can provide detection to the known and unknown malware threat with less false alert [18][19].	Revealing pattern from large amount of resources. Precision and accurate decision.	Poorly design AI could create false interpretation when input is false.
	Firmware Vulnerability	AI provide IoT device with smart vulnerability and patch management that proactively prevent firmware vulnerability by providing automated scan on the devices.	Handling repetitive task without any weaknesses.	Poorly design AI could result in poor decision.
Device Layer	IoT Device Capability	AI can monitor unwanted processes and detect anomaly in the power or memory consumption pattern.	Monitoring and processing can be done 24/7.	Devices need to have high processing resources.

IV. Potential Impact of Recent Advancements nn IoT

This section provides foresight and in-depth analysis which facilitates the exploration and improve understanding of the potential impact of recent advancements in the Internet of Things (IoT). This further discussion presents the expected and unexpected impacts that could arise from the development and the adoption of the technology to various areas such as military, law enforcement and intelligence. The discussion also includes anticipatory law-making considering the legislative issues/policies/standards which are useful for policy makers and legislators.

A. Smart Transport

1) Expected impacts: One of the advancement is electric vehicles, an important means of reducing fuel costs. A number of studies have investigated the functions and performance of the lithium-ion battery in electric vehicles. Autonomous vehicles have the capacity to be operated automatically without human intervention and integrated with parking infrastructure to produce a 'driverless parking system' accessible through smartphones [20]. Automated and connected vehicles are able to navigate to destinations and interact with other vehicles and objects effectively, leading to vast improvements in traffic flow. With increased connectivity, vehicle performance monitoring such as fuel efficiency and safety can be improved significantly. Moreover, the IoT has been used in train maintenance [1]. Numerous onboard and ground-based sensors transform the maintenance from corrective/reactive activities to a system that reflects the real conditions of each train's components. The collected data is used for analysis and decision making in near real time.

2) Unexpected impacts: In the case of an autonomous and driver-less vehicle, it is essential for policy makers and legislators to re-explore the definition of a 'responsible driver', which presently refers to the responsibility that lies with human drivers of vehicles. However, because autonomous vehicles can be operated automatically and by all members of society such as young children, the concept of 'responsible driver' might be different. It is also important to consider the implications for personal driving skills and road safety. Probably, a new set of IT skills is required in addition to a practical ability to drive and operate the vehicle. In considering the legislative issues, it is important to address topics such as liability for damages, data security and protection, and quality standards. Regulatory bodies need to ensure appropriate standards are adhered to for smart vehicles.

B. Defence and Public Safety

1) Expected impacts: A significant development in this area is the use of drones by both military and civilian authorities for core duties of safety, security and policing, particularly in carrying out surveillance and intelligence gathering. The immediate impact of this will be to reduce the numbers of personnel being deployed in carrying out these activities, and, in the future, drones could be seen carrying out dangerous activities such as assisting in eliminating forest fires. Drones are most visibly used for military purposes but they also have many other applications, such as mapping and logistics. Drone technology costs are expected to drop in the short term [20] and this makes it likely that there will be a widespread increase in their use by the public.

2) Unexpected impacts: There are significant legal and ethical issues associated with the increased use of drones. The usage of commercial and public drones is expected to impact significantly upon the safety and security of the public as well as having serious implications for public privacy. There is a societal impact of drones, the 'fear of being watched', which might influence the behaviour of citizens in public spaces. Another implication is personal privacy, particularly as drone users are allowed to take photographs or videos. A number of issues like access and sharing of data also exist. The impact of substituting community policing with a greater use of drones, for instance, risk of unemployment, lack of human values in

its operation and psychological impact on innocent civilians, and also the skills and traits–such as the IT technical and interpersonal skills needed for 'remote policing'–should be considered as well. There is the potential for clashes in the use of airspace between drones and both military and civilian aircraft. This conflict needs to be resolved, through devising policy and rules to safeguard the drones whilst upholding military and commercial priorities. The impact of safety is huge if a drone is taken over for destructive usage.

From another perspective, existing connected devices in the IoT-enabled applications and services pose disruptive challenges for national defence authorities because IoT devices present new kinds of targets, as well as new weapons to threaten economic and physical security [21]. These challenges are hard to address with traditional defence policy as both targets and weapons are often owned and operated by private entities. A sound cyber defence policy enables timely and decisive actions at each level of cyber operation. Thus, policy makers should provide standard policies and useful frameworks for analysis.

V. The Geopolitics of IoT Adoption

A. Geopolitical Risk and Threats

IoT devices present a new kind of threat and may be used as a weapon and target for cyber attackers to topple geopolitical stability. The most frequent cyberattacks reported are DDOS, MITM, phishing, and cyberespionage. Cyberattack techniques may vary, depending on the severity of damage intended by the attacker. With the rise of the IoT, many objects and devices are in danger of being part of thingsbot, which are botnets that incorporate independent connected IoT devices.

In recent years, IoT devices have often been used as weapons, where the malicious actors take control of connected devices to perform a cyberattack. Many cases of data and identity theft through hacked vehicles and hacked smart refrigerators have been previously reported. In 2014, a Samsung smart refrigerator, RF28HMELBSR, was a target of a man-in-the-middle attack to steal victims' Google credentials [22]. The hacking of Jeep Cherokee in July 2016 through MITM attack has also enabled hackers to access and control the vehicles' basic functions and consequently endangered the human life.

IoT devices may also be exposed as a target. A targeted attack on large IoT systems and critical infrastructure (e.g. power, water, national defence and security) may cause huge damage and disruption of service on a larger scale, particularly in smart buildings, smart cities and industrial control systems (ICS). In the past, the SCADA systems in ICS are 'air-gapped' to safeguard the systems. However, with the progress of Industrial IoT (IIOT) and networked integration across SCADA systems [23], the systems are often controlled by operating systems such as Windows and Linux, thus exposing the systems to mainstream malware.

B. Geopolitical Issues and Adversaries

Cyberattacks are often connected to geopolitics whether they originate from state or non-state actors. A state actor often operates under some degree of political direction and interests. The cyberattacks are often sophisticated and tend to project moderate disruptive or destructive cyber force due to instruments of deterrence. Examples of state threat actors are militaries, foreign intelligence services and state-sponsored hackers. Non-state threat actors include hacktivists, terrorists and jihadists, who often operate beyond legal jurisdictions [24]. Table 3 provides a comparative analysis of the associated geopolitical risk arising from related IoT threat incidents.

TABLE III. Comparative Analysis of the Associated Geopolitical Risk

Issues	Interest Involved	IoT Threat Incidents	Incident Detail	Associated Geopolitical Risk
Increasing political friction with the US over the Iranian nuclear program.	US, Israel, Iran	2012-Natanz uranium enrichment facility	Method: Stuxnet botnet IoT Weapon: Siemens SCADA systems [25]. Damage: 1,000 gas centrifuges in the Natanz facility.	Stuxnet succeeded in briefly setting back the Iranian nuclear programme. The attack has set a precedent for cyberwarfare, in which other countries launch digital assaults to resolve political disputes.
	Iran hack-tivist, US	2013-New York Dam attack	Method: Google dorking IoT Target: Flood-control systems for approximately 3 weeks. Damage: None as the dam was shut down during the attack	Given that there are 7,500 dams and 6,000 electric utilities in the US with potentially millions of IoT devices, the potential geopolitical risk meant to undermine US national security is substantial[1].

[1] E. Larson, P. Hurtado, and C. Strohm, "Iranians hacked from Wall Street to New York dam, US says," Bloomberg, 24 March 2016, https://www.bloomberg.com/news/articles/2016-03-24/us-charges-iranian-hackers-in-wall-street-cyberattacks-im6b43tt

Issues	Interest Involved	IoT Threat Incidents	Incident Detail	Associated Geopolitical Risk
Russian military intervention in Ukraine	Russia, Ukraine	2015-Ukraine Power Grid Attack	Method: Spear-phishing using "BlackEnergy" Malware IoT Target: SCADA systems Damage: Power outage for 230,000 consumers.	The attack can be seen as part of Russia's hybrid war strategy [26] that is to strengthen Russia's political position in the Baltics, Central Europe, and the EU. The attack is significant to demonstrate a deterrent to other Baltic states with desynchronization aspirations, and undermine societal and economic reputation of the Baltic states' government.
		2016-Kiev Substation Attack	Method: Industroyer malware IoT Target: controlling critical equipment directly like electricity substation switches and circuit breakers Damage: Power outage in Kiev	
South China Sea dispute	China, US, Philippine	2016-Illegal seizure of US underwater drone	IoT Target: US UUV	The illegal seizure of a US vessel in violation of sovereign immunity. Moreover, the Chinese warship violated high seas freedoms of the USNS Bowditch under the United Nations Convention on the Law of Sea.
	China, Brunei, Malaysia, Philippine Taiwan, Vietnam, US	2018-Building of largest test-site for unmanned vessels in Zhuhai, China	IoT Weapon: Unmanned system	China's action may assert sovereignty over the South China Sea. This can be seen as a potential means for remote patrol and enforcement of the Chinese territorial claim in the South China Sea[2].
Fears of China cyberespionage	China, US	2017-US army bans Chinese products	Method: Backdoor IoT weapon: Hikvision's cameras, DJI drones Damage: Cyber-espionage	In the interest of increasing cyber deterrence, the US may object more to the behaviour of some other nations in cyberspace and may aim to impose costs on adversaries [27].
		2018-US to ban ZTE from using US technology for 7 years due to illegal shipping to Iran and N. Korea.	Method: Backdoor IoT weapon: ZTE smartphones Damage: Data theft	
Korean Peninsular conflict	North Korea, South Korea	2016-Hacking of South Korea government officials' smartphones.	Method: Cyber vulnerabilities/backdoor IoT weapon: Smartphones Damage: Data and identity theft	Data and identity theft could be used for identifying targets for potential defectors, or target for assassination to support North Korea's political objectives.

[2] N. Chandran, "Beijing is using underwater drones in the South China Sea to show off its might," CNBC, 15 May 2014, https://www.cnbc.com/2017/08/12/china-uses-underwater-drones-in-south-china-sea.html

C. Case Study

1) Chinese naval expansion in the south china sea: To improve understanding on the geopolitical implication of IoT adoption, this section presents a discussion on the roles that China sees for Unmanned Vehicle (UV) [28] technology because of its relevance to maritime territorial disputes in the South China Sea. UV technology highlights a number of growing roles in monitoring territorial disputes at sea that include intelligence, surveillance and reconnaissance (ISR), maritime surveillance, disaster relief, combat application missions, and military communication relay capabilities [29]. The biggest advantage of using a UV in the South China Sea is the absence of human operators, making it ideal for high-risk missions. In these contested waters, a UV can be more effective, convenient and safe than manned systems involving human operation on location[3], enabling the UV to be used in more assertive ways and making it more appropriate for hybrid warfare.

Since the Scarborough Reef incident in 2012, China has deployed unmanned vehicles over disputed territory. In May 2016, China's BZK-005 surveillance drone was spotted on Woody Island, and the same drone was used in the East China Sea, causing a political dispute between China and Japan. In the same year, China was working on a project called Underwater Great Wall[4] that would give Beijing information about vessel movement in the South China Sea. In response to China's continued sovereignty assertiveness in the South China Sea, the Philippines approved a defence cooperation deal with the United States in January 2016 to assist the Philippines in modernizing its military forces. In December 2016, a Chinese warship seized a US unmanned underwater drone (UUV) for marine research purposes[5] within the Philippines exclusive economic zone (EEZ).

The case offers several significant geopolitical implications. The biggest concern is for the conflicting countries and international community who use the South China Sea route for trade purposes. A nation that can monitor the maritime trade of another country might be able to see new vulnerabilities in that other country's economy. As more nations shift towards ISR for military surveillance to gather intelligence about enemy, a nation can deploy its navy or in the case of war launch a surprise attack. Moreover, following the US UUV seizure incident, Beijing made a legislative move that requires all foreign submersibles to travel on the water surface when in China's claimed territorial waters[6]. This move seems to reduce US ISR assets in the South China Sea and to mitigate US military presence in the Asia-Pacific region.

2) Autonomous vehicles for consumers: The proliferation of ascendant technologies such as AI and machine learning opens new opportunities enabled by AI including autonomous vehicles (AVs). A report [30] by the Brookings Institute showed that approximately $80 billion has been spent on AV technology development from 2015 to 2017. Starting from 2015, a full automation vehicle has been developed for AV. McKinsey predicted that AVs would become the primary means of transport in 2050 [31]. However, despite a positive directional trend for AVs, consumers still doubt the safety of and associated risks with AV technology [32].

Hence, several potential geopolitical implications of the AV technology have been analyzed which might present barriers towards the adoption of this technology. As the AV may reduce environmental pollution, several countries like Norway, Britain, France and the Netherlands have announced their plan to ban gas and diesel cars by 2040[7]. Increased reliance on lithium-ion batteries will significantly reduce the demand for oil, thus causing oil to suffer a price drop [33]. The decline in oil demand will largely impact oil-dependent countries with small financial safety nets such as Venezuela, Libya and Nigeria. As a result, internal and external political instabilities may emerge in the affected countries. However, the reverse effect should be expected for net importer countries.

With the advancement of the AV technology, there will be a high possibility that AVs will be used as cyberweapons to perform attacks. Such attacks may be directed against an individual or on a larger scale, against a country. For example, the hacking of an AV system may enable state-sponsored hackers to access and control the vehicle to perform an assassination operation. The potential for remote attacks through hacked vehicles will be deemed lucrative for terrorists, particularly for jihadists, where suicide attacks as seen in the 2016 Nice attack will no longer be necessary. Finally, the adoption of AV technology may change the business condition particularly for global logistics and public transportation. The role of the human driver may cease, as companies such as Uber and Lyft have conducted tests and evaluations on the applicability of AV technology in their operations. In the US, Goldman Research estimates that when autonomous vehicle saturation peaks 25,000 occupation losses per month[8] particularly for truck, bus and taxi drivers when autonomous vehicle saturation peaks.

[3] T. Burgers and S. N. Romaniuk, "Will Hybrid Warfare Protect America's Interests in the South China Sea?," March 30, 2017, The Diplomat, https://thediplomat.com/2017/03/will-hybrid-warfare-protect-americas-interests-in-the-south-china-sea/

[4] S. Bana, "China's Underwater Great Wall", Washington Times, 30 August 2016, https://www.washingtontimes.com/news/2016/aug/30/chinas-underwater-great-wall/

[5] H. Agerholm, "China seizes US Navy underwater drone in international waters of South China Sea," Independent, 16 December 2016, https://www.independent.co.uk/news/world/asia/china-seize-us-navy-underwater-vehicle-south-china-sea-one-china-taiwan-a7480016.html

[6] "China considering making foreign submersibles travel on surface," Reuters, 15 February 2017, https://www.reuters.com/article/us-china-defence/china-considering-making-foreign-submersibles-travel-on-surface-idUSKBN15U0QR

[7] A. Petroff. These countries want to ban gas and diesel cars. CNN.11 September 2017. http://money.cnn.com/2017/09/11/autos/countries-banning-diesel-gas-cars/index.html

[8] A. Balakrishnan, "Self-driving cars could cost America's professional drivers up to 25,000 jobs a month " CNBC, 22 May 2017, https://www.cnbc.com/2017/05/22/goldman-sachs-analysis-of-autonomous-vehicle-job-loss.html

VI. Strategic Considerations for Geopolitical Risk Mitigation

A. International Cooperation and Responsibility

The responsibility for ensuring mitigation of geopolitical risks relating to the IoT requires international collaboration across governments and international organizations. Continuous development and international agreements on behaviour in cyberspace may promote stability in cyberspace in the long run [27]. The most important international agreement to date relating to the protection of society against cybercrime is the Budapest Convention on Cybercrime (2001). In combatting IoT botnet threats, in 2013 the Cybercrime Convention Committee (T-CY) issued guidance notes [34] that state botnets fall within the Convention's remit because "the computers in botnets are used without consent and are used for criminal purposes and to cause major impact". In June 2017, the Cybercrime Convention Committee agreed to draft a second additional protocol to further expand the scope of the Budapest Convention [35], which enables access to electronic evidence in the cloud and more effective mutual legal assistance. If adopted, it may facilitate international investigation to identify the perpetrators of an IoT attack. However, these efforts are not as effective since some of the key players in the IoT market such as China, Russia and India are not part of the Convention, hence the need for a universal treaty at United Nations (UN) level.

In the absence of a universal treaty on cybercrime, the other options are to pursue regional cooperation and to pursue bilateral agreement regarding responsible behaviour in cyberspace. Some notable regional cooperation is seen in the Shanghai Cooperation Organization for Northeast and Central Asia (2009) and the African Union Convention on Cybersecurity and Data Protection (2014). On another hand, some countries have attempted to establish cooperation on a bilateral basis to mitigate cyber threats. For example, China and the United States are committed to refrain from conducting economic cyberespionage between the two nations as part of a cybersecurity agreement made in September 2015. As a consequence, a decrease in hacking activities originating from China has been observed [36]. Similarly, China has signed multiple bilateral cybersecurity agreements with Russia (May 2015) and Australia (April 2017), and pursued high-level cybersecurity dialogue with Germany (November 2016) and Canada (May 2017).

Finally, organizations and industry have an increasing role to play in addressing geopolitical risk. At present, standardization across the IoT security landscape is fragmented and needs alignment in its development. Several industry alliances have shown international efforts to deliver an interoperable IoT infrastructure and secure information flows. In 2015, high-tech industry companies and notable academic institutions formed the OpenFog Consortium with the aim being to establish global security and privacy reference architecture for Fog Computing. In September 2016, the IIC members published the Industrial Internet Security Framework (IISF) [37] that aimed specifically to create broad industry consensus for securing IIoT systems and to promote IIoT security best practices within business and industrial operations.

B. Laws and Regulations

Currently, there are at least two main regulatory frameworks that apply to the geopolitical risk of IoT, including data protection regulations and security of essential service [23]. Due to geopolitical uncertainty, many countries have imposed laws and regulations that tighten cross-border data flow and technology equipment. Such decisions are driven by data localization requirements, enforcing how data can be collected, processed and stored within a country. For instance, the EU General Data Protection Regulation (GDPR) places conditions on permitting EU residents' personal data to be transferred only when an adequate protection level is met. Under GDPR, geolocation data that is usually collected and stored in IoT devices is also protected.

With the increasing number of cyberattacks against critical infrastructures and IIOT, the EU Network and Information Security (NIS) Directive (2016) sets out a common EU cybersecurity framework to prevent and minimize the impacts of cyberattacks on EU member states' interconnected infrastructure. Articles 14 and 15a in the NIS Directive define the minimum obligations required from critical service operators and digital service providers to share information on cyberattacks among member states. In addition, the organization is required to report cyberattack incidents to computer security incident response teams (CSIRTs) when minimum threshold harm is met.

At a domestic level, China's National Cybersecurity Law (2017), for instance, has tightened and centralized state control over the flow of internet data and technology equipment, and prevents other network security violations. Critical information infrastructure operators are required to store their data within its national border, and help the Chinese government decode the encrypted data, if necessary [38]. Additionally, the law imposes mandatory security assessment on technology equipment and cross-border data transfer. Similar data localization requirements can be seen in Russia's Yarovaya Law (2016). These requirements represent a new challenge to foreign companies that do business within its borders [38], and may affect companies' competitiveness and undermine access to competitive services.

C. Role of Industry and Governmental Positions

This section covers role specification of multiple industry and governmental positions, such as technology modellers, policy makers, cyber security professionals, and state planners (Table 4). Emphasis will be given to the importance of cooperation among different individuals involved in the technology adoption.

TABLE IV. EXAMPLES OF ROLE SPECIFICATION

Position	Type (Industry/ Government)	Role
Policy maker/Device manufacturer	Industry	Involved in IoT Trustworthy Working Group and establishing a certification programme among manufacturers of IoT devices to follow the same IoT standard that will increase interoperability and quality [39].
IoT architect	Industry	Responsible for engaging and collaborating with stakeholders to establish an IoT vision and objectives, design an IoT architecture and establish processes for constructing and operating IoT solutions [1].
Policy maker/ State regulator	Government	Establishment of data protection law [39], provide guidance and management procedures in responding to cyberattacks and act as lead agency for intelligence support [20].
Device developer	Industry	Follow the guidelines provided in the standard framework to enhance the security and privacy of devices, (for example home devices, wearable fitness and health technologies) and the collected data.
Enterprise architect	Industry	- Adopt ideation-based approaches to exploit the IoT's potential. - Create business scenarios for the use of IoT technologies. - Manage risks by devising IoT information architecture, partner with other roles to develop an interoperability strategy. - Focus on providing IoT experiences users want.
Data scientist	Industry	- Support operational decisions, facilitate innovation by providing insights into how products and services are being used and can be improved. - Analyze data and create digital models to convert huge amounts of data into decisions and actions.
Police officers	Government	Law enforcement and protection of the citizens: keep the peace and secure volatile areas, prevent and investigate crimes, detain individuals suspected/ convicted of offenses against criminal law. Urban or rural environments, major events and border areas.

VII. CONCLUSION

Improving the stability of cyberspace in the face of insecure IoT technologies requires a combination of effective technical and regulatory approaches. This brief presents the analytical gaps identified with respect to the potential use of ascending technologies in addressing IoT security concerns and the gaps in current IoT security solutions. A comparative assessment that illustrates the expected and unexpected impacts of the technology adoption and the associated geopolitical risk arising from related IoT threat incidents is presented. This brief provides gaps to guide the government, industry and research community in pursuing future technological development that may be in need of improvement. The advancement in technological development requires appropriate alignment by all parties to improve resilience in the face of the increased risk of IoT threats and to mitigate the risks associated with such threats.

ACKNOWLEDGMENT

This paper is funded by Global Commission on the Stability of Cyberspace (GCSC) Grant (GLUAR/HGCC/2018/FTMK-CACT/A00015). A high appreciation to Fakulti Teknologi Maklumat dan Komunikasi, niversiti Teknikal Malaysia Melaka (UTeM) for facilitating the work done in this paper.

REFERENCES

[1] M. Hung, "Leading the IoT: Gartner Insights on How to Lead in a Connected World.", Gartner, 2017.

[2] S. Pallavi, and S. R. Sarangi. "Internet of things: architectures, protocols, and applications." Journal of Electrical and Computer Engineering 2017.

[3] R. Ammar, and S. Samer. "Internet of Things—From Hype to Reality." The road to Digitization. River Publisher Series in Communications, Denmark 49, 2017.

[4] S. Zhengguo, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung. "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities." IEEE Wireless Communications, vol. 20, no. 6, pp. 91-98, 2013.

[5] M. Rwan, T. Yousuf, F. Aloul, and I. Zualkernan. "Internet of things (IoT) security: Current status, challenges and prospective measures." In Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference, pp. 336-341, 2015.

[6] S. Sachchidanand, and N. Singh. "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce." In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, pp. 1577-1581. IEEE, 2015.

[7] Z. Zhi-Kai, M. Cheng Yi Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh. "IoT security: ongoing challenges and research opportunities." In Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on, pp. 230-234. IEEE, 2014.

[8] X. Teng, J. B. Wendt, and M. Potkonjak. "Security of IoT systems: Design challenges and opportunities." In Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design, pp. 417-423. IEEE Press, 2014.

[9] L. Qi, Y. C. Hu, and X. Zhang. "Even Rockets Cannot Make Pigs Fly Sustainably." In Workshop SENT'14, 23 February 2014, San Diego, USA, Copyright 2014 Internet Society: Proceedings. Internet Society, 2014.

[10] V. Rijswijk-Deij, A. S. Roland, and A. Pras. "Making the case for elliptic curves in DNSSEC." ACM SIGCOMM Computer Communication Review, vol. 45, no. 5, pp. 13-19, 2015.

[11] J. McCarthy, "Artificial intelligence, logic and formalizing common sense." In Philosophical logic and artificial intelligence, pp. 161-190. Springer, Dordrecht, 1989.

[12] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. "Blockchain for IoT security and privacy: The case study of a smart home." In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on, pp. 618-623. IEEE, 2017.

[13] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar. "Quantum cryptography for IoT: APerspective." In IoT and Application (ICIOT), 2017 International Conference on, pp. 1-4. IEEE, 2017.

[14] M. J. O. Saarinen, "Ring-LWE ciphertext compression and error correction: Tools for lightweight post-quantum cryptography." In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, pp. 15-22. ACM, 2017.

[15] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi. "Securing the Internet of Things in a quantum world." IEEE Communications Magazine, vol. 55, no. 2, pp. 116-120, 2017.

[16] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control." Journal of medical systems, vol. 40, no. 10, pp. 218, 2016.

[17] P. Ghuli, U. P. Kumar, and R. Shettar. "A Review on Blockchain Application for Decentralized Decision of Ownership of IoT Devices." Advances in Computational Sciences and Technology, vol. 10, no. 8, pp. 2449-2456, 2017.

[18] T. N. Brooks, "Survey of Automated Vulnerability Detection and Exploit Generation Techniques in Cyber Reasoning Systems." arXiv preprint arXiv:1702.06162 (2017).

[19] H. Tagato, Y. Sakae, K. Kida, and T. Asakura, "Automated Security Intelligence (ASI) with auto detection of unknown cyber-attacks." NEC Technical Journal, vol. 11, pp. 45-48, 2016.

[20] L. Van Woensel, L. G. Archer, L. Panades-Estruch, and D. Vrscaj. "Ten technologies which could change our lives: Potential impacts and policy implications." depth analysis, 2015.

[21] R. Arashi, L. F. Pedersen, A. Hillock, S. Jones, J. Midgley,J. Pelczar, G. Rickert, and L. W. Cahili, "Defense Policy and Internet of Things Disrupting Global Cyber Defenses." Deloitte, 2017.

[22] Z. Cekerevac, Z. Dvorak, L. Prigoda, and P. Cekerevac. "Internet Of Things And The Man-In-The-Middle Attacks–Security And Economic Risks." Journal (MESTE), vol. 5, no. 2, pp. 15-25, 2017.

[23] L. Urquhart, and D. McAuley. "Avoiding the internet of insecure industrial things." Computer Law & Security Review, vol. 34, no. 3, pp. 450-466, 2018.

[24] J. Sigholm, "Non-state actors in cyberspace operations." Journal of Military Studies, vol. 4, no. 1, pp. 1-37, 2013.

[25] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security." In IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society, pp. 4490-4494. IEEE, 2011.

[26] H. Bahsi, A. Bulakh, T. Jermalavičius, A. Petkus, and N. Theisen. "The Geopolitics of Power Grids–Political and Security Aspects of Baltic Electricity Synchronization.", 2018.

[27] Price Waterhouse Coopers, "The Global State of Information Security Survey, 2017." Price Waterhouse Coopers, 2017.

[28] Z. Tian, L. Fushun, Z. Li, R. Malekian, and Y. Xie. "The development of key technologies in applications of vessels connected to the internet." Symmetry vol. 9, no. 10, pp. 211, 2017.

[29] C. C. Kao, Y. S. Lin, G. D. Wu, and C. J. Huang. "A Comprehensive Study on the Internet of Underwater Things: Applications, Challenges, and Channel Models." Sensors, vol. 17, no. 7, pp. 1477, 2017.

[30] C. F. Kerry, and J. Karsten. "Gauging investment in self-driving cars." Brookings Institution, October 16, 2017.

[31] M. Bertoncello, and D. Wee. "Ten ways autonomous driving could redefine the automotive world." McKinsey, 2015.

[32] C. A. Giffi, J. Vitale Jr, T. Schiller, and R. Robinson. "A reality check on advanced vehicle technologies." Insights exploring new automotive business models and consumer preferences, p. 8, 2018.

[33] J. Arbib, and T. Seba. "Rethinking Transportation 2020-2030." RethinkX, May, 2017.

[34] Cybercrime Convention Committee, "(T-CY) Guidance Note #2 Provisions of the Budapest Convention covering botnets", 5 June 2013.

[35] "Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime". Cybercrime Convention Committee (T-CY), 1 June 2017.

[36] iSIGHT Intelligence, FireEye. "Red line drawn: China recalculates its use of cyber espionage." FireEye, 2016.

[37] Industrial Internet Consortium. "Industrial Internet of Things Volume G4: Security Framework. Industrial Internet Consortium.", 2016.

[38] Cory, Nigel. "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?." Information Technology and Innovation Foundation (ITIF), 2017.

[39] Pawel, T. "Application of Internet of Things in Logistics-Current Challenges." International Society of Manufacturing, Service and Management Engineering, no. 7, pp. 54-64, 2015. 47