RCGCG
网络空间国际治理研究中心
RESEARCH CENTER FOR GLOBAL CYBERSPACE GOVERNANCE

ioXt
internet of secure things

White Paper on 2022 Global IoT Security

White Paper on 2022 Global IoT Security

Research Center of Global Cyberspace Governance (RCGCG)
ioXt (Internet of Secure Things Alliance)

July, 2022

Preface

IoT (Internet of Things) security poses a major challenge to global cybersecurity. Many risks emerge, such as IoT device security, data security, and personal privacy protection, which necessitate enhanced security guarantees in terms of product design, technological standard, compliance certification and security governance. Simultaneously, IoT security is undermined by Sino-US technology decoupling, which intensifies with geopolitics, national security and other factors. These complex factors have impeded the improvement of global IoT security. In order to investigate the issue in a more comprehensive way, Research Center of Global Cyberspace Governance (RCGCG) in collaboration with ioXt (Internet of Secure Things Alliance), a research institution on cybersecurity policy and technological standard, has published White Paper on 2022 Global IoT Security; PSA Certified, a global partnership of security-conscious companies, also contributed to part of the content.

Members of the research group include Lu Chuanying, researcher from Shanghai Institutes for International Studies (SIIS); Wang Li, senior researcher from Xi´an Jiaotong University Suzhou Academy Information Security Laws Institute; Hui Zhibin, researcher from Shanghai Academy of Social Sciences; Lang Ping, researcher from Institute of World Economics and Politics, Chinese Academy of Social Sciences; Xu Longdi, associate researcher from China Institute of International Studies (CIIS); Sun Xiantang, senior engineer from China Academy of Information and Communications Technology (CAICT); Craig Miller, director of Intellectual Property of ioXt; Dylan Liu, head of Business Development in Asia Pacific of ioXt, a leading organization in the field of global IoT standards; and Anurag Gupta, Director of Business Development of PSA Certified at Arm.

In the process of compiling the White Paper , the research group has initiated extensive academic exchanges with experts and scholars with profound insights in the fields of cybersecurity, Sino-US science & technology and cited their latest research achievements in this regard. Experts and scholars are Bruce McConnell, distinguished fellow at The Stimson Center; Paul Triolo, senior vice president from Albright Stonebridge Group (ASG); Graham Webster, senior researcher from Stanford University´s Cyber Policy Center (SUCPC); and Samm Sacks, senior researcher from Yale Law School.

Additionally, the research group has co-organized relevant academic seminars with John C. Mallery, researcher from Massachusetts Institute of Technology (MIT)、Joseph Nye, professor at Harvard Kennedy School, Melissa Hathaway, senior advisor at Harvard Kennedy School, and Charles Barry, former professor at National Defense University, attended seminars and discussed IoT security deeply. Their penetrating views possess great significance for better understanding global cybersecurity development and boosting global IoT security.

Abstract

The key technologies of IoT are quickly maturing, the optimization of IoT deployment costs continuously advancing, and the demand for IoT applications are constantly evolving. Under such circumstances, IoT plays a positive role in promoting the integrated development of the digital economy and the real economy, and facilitating industrial transformation & upgrading, digital-consumption level, and urban service capacity. The era of IoT and IoE (Internet of Everything) has arrived.

Against the backdrop of the wide coverage of IoT devices and the deep integration of IoT industrial applications, IoT security deserves our great attention. There are a huge amount of terminal devices at the perception layer and varying security-protection capacities, easily becoming a springboard for cyberattacks. Traditional communication security and new risks & challenges at the network layer interweave or overlap, which can harder to counteract targeted attacks. The integration of IoT systems and business systems at the application layer probably enlarges risk exposure. In the digital era, IoT security involves major matters of personal privacy, business data, social management, economic development, and national security.

To establish the basic system of IoT security guarantee and improve the security level of IoT industrial applications, various countries have released laws, policies, and guidelines on IoT security. The United States protects the security of the network and key infrastructure of the federal government via executive order and legislation. It determines the cybersecurity-capability baseline of IoT devices with NIST standards and guidelines. While highlighting the protection of personal privacy and enhancing the security of the IoT supply chain, the European Union emphasizes that the security baseline of software security covers the lifecycle of IoT products and services. China accelerates the construction of IoT security-guarantee system from multiple aspects of top-level planning, laws & regulation, and standard formulation, and forges a favorable environment for the development of the IoT industry. International organizations represented by the United Nations, the International Organization for Standardization (ISO), and the International Telecommunications Union (ITU) establish standards on security in emerging fields like security-system framework with the principles

of standard, regulation, and security, which guide and improve IoT service quality and security level in the world.

Globally, countries are working to strengthen the governance of IoT security. IoT enterprises face significant challenges in compliance. Policies on cybersecurity are being tightened, and the legal boundaries are expected to be clarified. The complexity of IoT technology increases the costs of corporate compliance. The inexorable structural collision between the existing regulatory policies of governments and the rapid evolution of new technologies necessitates the scrutiny of supply chain security based on the generalized idea of national security. It further inhibits the collaborative global development of IoT security.

To quicken the construction of IoT-security systems and improve the governance level of IoT security, the White Paper proposes relevant suggestions in order to enhance public confidence, advance governance efficiency, protect the enthusiasm of IoT enterprises, and deepen the rapid evolution and development of the global digital economy with IoT economy.

Contents

Chapter 1

Overall Situation of Global IoT Security 1

1. IoT Security Faces A Complex Landscape 1
2. Cybersecurity in IoT Layered Architecture 3
3. Main Factors That Influence IoT Security 6

Chapter 2

Overview of Global IoT Security Governance 10

1. National Level: Top-Down Policy Layout for IoT Security 10
2. Market Level 20
3. International-Organization Level 23

Chapter 3

Main Challenges to IoT Corporate Compliance 32

1. Increasingly Stringent Cybersecurity Policy and Blurry Legal Boundary 32
2. Technological Complexity Increases Compliance Costs 37
3. The Contradiction between Outdated Policies and the Application of New Technologies 43
4. Geopolitical Games Complicating the Landscape of IoT Security 46

Chapter 4

The Best Practices of IoT Security 51

1. IoT Security Certifications 51
2. Case Studies 53

Chapter 5

Initiatives to Safeguard Global IoT Security 60

Chapter 1

Overall Situation of Global IoT Security

Today, as new technologies and applications such as 5G, AI and edge computing are applied in the IoT industry, and IoT devices are rolled out into the fields of smart grid, logistics, and medical care, the era of IoT or IoE is at hand. IoT and IoE have wide-reaching impacts on public life, social governance, national politics, and economic security. In 2021 and 2022, Groupe Speciale Mobile Association (GSMA), an international think tank, released The Mobile Economy 2021 and The Mobile Economy 2022, suggesting that the total number of global IoT connections reached 13.1 billion in 2020[1] and 15.1 billion in 2021 and that the number of global wired IoT devices will reach 23.3 billion by 2025. Relevant data predicts that the total value of the global IoT market in 2020 reached 389 billion US dollars and will grow to one trillion US dollars in 2030.[2]

1. IoT Security Faces A Complex Landscape

IoT technologies not only actualize the digital and intelligent development of reality, but also pose non-negligible risks.

First, in terms of application, IoT key devices cover civil life and critical information infrastructure, and affect wide fields. IoT involves critical information infrastructure industries like power grids, transportation, and medical care. Meanwhile, autonomous vehicles and intelligent medical devices are closely related to public life. These fields develop rapidly, which makes cybersecurity more complex. Cyberattacks that target industrial IoT systems like the power grid, water plants and intelligent manufacturing set off serious incidents like power outages, uncontrollable traffic, and factory shutdown. For instance, the WannaCry Ransomeware attack began in May 2017. It wreaked havoc on British hospital and clinic systems, resulting in the cancellation of more than 20,000 appointments and the closure of a Renault factory, the French carmaker.[3]

1.GSMA. The mobile economy 2021[EB/OL].[2021-06]. https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/06/GSMA_MobileEconomy2021.pdf
2. FinancesOnline.35 IoT Device Statistics You Must Read: 2022 Data on Market Size, Adoption & Usage[EB/OL].https://financesonline.com/iot-device-statistics/
3. https://www.aqniu.com/. “From Ukrainian Power Grid to German Steel Plant: Five Real Cases of Attacks on Industrial Control System [EB / OL]. [2018-05-11] .https://www.secrss.com/articles/2598.

Attacks on home automation systems such as heating, air conditioning, and lighting cause severe inconvenience to public life. For example, with the development of the Internet of Vehicles, the importance of communication security for in-vehicle networks has become more apparent. If passengers unknowingly carry hacked devices and are connected to an internal vehicle network, Internet of Vehicles will face a great threat. Devices could send instructions to a vehicle via the in-vehicle network and gain control of a vehicle, threatening both safety and property.[1]

Second, in terms of product, overall IoT security ecology hardly takes shape among various forms of IoT products, with large security risk exposure. IoT products are diverse in form. Particularly, consumer-oriented terminal products such as cameras, intelligent wearable devices, Internet appliances, and baby monitors. The design of the aforementioned terminal devices mostly highlights the support of current usability, and the level of security-protection design varies. The uneven quality of IoT security products leads to the vulnerable foundation of IoT security.

Simultaneously, a large number of terminal devices are deployed in complex use cases, which can hardly guarantee the overall security of IoT applications. Furthermore, customers are negligent in altering passwords and reluctant to upgrade products. Consequently, terminal devices cannot effectively resist cyberattacks that constantly evolve. In 2016, a security vulnerability was exposed in British Owlet infant heart monitoring sensors. Anyone who stayed in the monitoring range gained access to monitor the infant's data, which disturbed the monitoring and alarm systems.[2]

Third, in terms of technology, cybersecurity risks against a background of the rapid development of IoT may amplify the risks. Noticeably, network infrastructure always faces complex and diverse risks. In 2018, IoT network infrastructure started to progress towards cross-technological integration and full-scene coverage. Mobile network (cellular IoT network and unauthorized IoT network), local area network, satellite network, unmanned aerial vehicle and hot-air balloon jointly build space-air-ground integrated network (SAGIN) global IoT network infrastructure.[3] IoT technologies embody varying degrees of maturity, and cybersecurity faces more complex and diverse problems.

When IoT relies on network and cloud in transmission, processing, and storage, the universality of application and the immaturity of technology coalesce, which may further amplify IoT security risks. In cloud computing, various security risks emerge, such as data leakage, configuration error, account hijacking, unsafe interface, and internal threats. Service usability, content security, and privacy protection need to be continuously strengthened. On January 11, 2021, Ubiquiti, a well-known IoT-device manufacturer whose products covered routers, IP cameras and security cameras, announced that it encountered illegal incidents, because its third-party cloud services were intruded, which resulted in the accidental outflow of a large number of customer-account

1. Xu Cheng. "Research on Mutual-Trust Authentication Protocol for Internet of Vehicles." [D] Beijing University of Posts and Telecommunications, 2019.
2. https://www.secrss.com/. "Research on Security Threats and Countermeasures of Medical Internet of Things." [EB/OL]. [2019-05-05]. https://www.secrss.com/articles/10409.
3. China Academy of Information and Communications Technology (CAICT). White Paper on Internet of Things (2020). [EB/OL]. [2020-12-10].

vouchers.[1]

Fourth, in terms of data, IoT wired devices widely collect data, which affects personal privacy, business secret and national security. Smart devices are deeply popularized and applied. Specifically, as smart home, smart car and smart government develop quickly, IoT data collection increasingly covers personal data privacy and industrial data like production and machine monitoring data. Personal data may involve privacy protection, and the aggregation and analysis of industrial data may involve the security of critical information infrastructure and even national security.

The security risk of data leakage exists in the lifecycle of IoT-data collection, transmission, storage, and processing. According to a report by Gizmodo, a technology and science media outlet, The Ulysses Group, LLC (Ulysses), a location intelligence platform based in the U.S., claims it can monitor the location information of vehicles in almost all countries except North Korea and Cuba, and that this data can be viewed "historically" or in real time. Ulysses believes the data will help the U.S. Federal Government conduct military intelligence operations more effectively.[2] Therefore, IoT-data security not only concerns personal privacy, but also poses a threat to national security with data aggregation and analysis.

Fifth, in terms of governance, a complex IoT supply chain makes it challenging to construct security systems. The diversification of security-responsibility subjects may incapacitate the fulfillment of emergency response and repair measures for the first time. IoT implicates many providers, e.g. chip, sensing technology, operating system, and operator, which stay at different layers of perception, network, platform, and application. The diversification of security-responsibility subjects and the lack of constraints on IoT security-system architecture obstruct the establishment of a reliable prevention mechanism for IoT security and the timely and appropriate emergency response in the face of high-intensity attacks.

2. Cybersecurity in IoT Layered Architecture

As the number of Internet devices soars, the volume and complexity of cybersecurity threats is also on the rise. Compared to traditional Internet models, IoT encounters more complex cybersecurity risks and challenges owing to its multi-source heterogeneity, openness and ubiquity.[3]Kaspersky reported that from January to June 2021, 1.51 billion IoT-device intrusions occurred, more than doubling from 639 million in 2020.[4] Cybersecurity turns out to be a major obstacle to the extensive deployment of IoT.

Currently, basic IoT architecture that is generally acknowledged mainly includes the percep-

1. Qing Lian Newsletter (No. 89). "On IoT Security." [EB/OL] [2021-04-06]. https://www.163.com/dy/article/G6UCIMLE0518V033.html
2. Lucas Ropek. This Surveillance Company Claims It Can Track Nearly Any Car in Real-Time[EB/OL]. [2021-03-17]. https://gizmodo.com/this-surveillance-company-claims-it-can-track-nearly-an-1846494534
3. Ant Security Lab. "Brief Analysis of Terminal Trusted Technology System in the Era of Internet of Things." [2021-11-09]. https://www.secrss.com/articles/35899.
4. Callum Cyrus,IoT Cyberattacks Escalate in 2021, [EB/OL]. [2021-09-17]. https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/.

tion layer, the network layer, the application layer, and the service-management layer, each of which has unique cybersecurity problems and interacts or mingles with other layers.

(1) Cybersecurity at the Perception Layer

The perception layer mainly comprises massive terminal devices and sensors. As the source of massive IoT data, its main function is to collect, identify and control all types of information of sensing objects in use cases. Structurally, basic components at the perception layer include sensor system, identification system, satellite positioning system, and corresponding information-supporting devices (e.g. computer hardware, server, network device and terminal device). Multi-source and heterogeneous terminal devices enable all kinds of IoT to contain more data on production and life information and personal privacy, which closely relate to business dealing, user privacy and national security, with the potential of small security breaches to cause massive chain reactions.

Terminal devices that form at the perception layer embody large scale and varying capacity. Besides, the security of most terminal devices is weakly protected, without the processing capacity of basic protection like encryption, thus becoming the disadvantage of the entire IoT security. In the meantime, terminal devices easily become a "springboard" for cyberattacks. Because of the large base, wide distribution and adequate network broadband resources, a large number of devices will be controlled in case of vulnerabilities, forming botnets and launching distributed denial of service (DDoS) attacks on network infrastructure. This results in service interruption and large-area network paralysis.[1]In 2016, the east coast of the United States suffered large-area network paralysis, which arouse from the strong DDoS attack on Dyn (Dynamic Network Services), an American provider for domain name resolution services. The attack traffic came from the terminal devices infected with Mirai botnet program.

(2) Cybersecurity at the Network Layer

The network layer performs IoT-node cooperation in local and short-range networks. Its function is to safely and efficiently transmit the data collected at the perception layer and mingle with the server. At the network layer, cloud, gateway, switch and router use wireless protocols, which comprise various private networks, Internet, wired and wireless communication networks and network-management systems. In an IoT system, the network layer acts as a transit hub for the entire IoT system.

The security risk at the network layer centers on communication security. Compared with traditional Internet, IoT protocols are diverse, with large attack surface. On the one hand, IoT devices are mainly based on embedded systems that take IEEE802 communication standards (e.g. ZigBee and Bluetooth) as the connecting model, with low costs and loose development environments. Device terminal-product manufacturers fail to conduct detailed security audits on the chip solution, development board, and operating system chip manufacturers provide. Consequently, vul-

1. China Academy of Information and Communications Technology (CAICT). White Paper on Internet of Things (2018). [R\OL]. [2018-09]. http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020180919390470911802.pdf.

nerabilities of original operating systems and components can be easily implanted into terminal devices and cannot be timely updated and repaired.

On the other hand, as the IEEE802 protocol-family is basically used for LAN communication with no end-to-end and overall security measures, security risks inevitably occur when the IEEE802 protocol-family provides the application of smart devices. Statistically, 98% of the traffic of connecting objects is unencrypted, and more than half of the devices are vulnerable to moderate or violent attacks.[1]

(3) Cybersecurity at the Application Layer

The application layer mainly includes application-support-platform sublayer and application-service sublayer. Specifically, the former is used to support the functions of information collaboration, sharing and interworking among different industries, applications and systems. The latter includes smart transportation, smart medical care, smart home, smart logistics, smart power and other industrial applications.[2]

It is a key challenge at the application layer to efficiently and intelligently process massive data and ensure the authenticity, integrity and confidentiality of data at the same time. Management interface, web API, Elastic Compute Service (ECS), system- function component and application-delivered services are vulnerable to attacks. Due to the scalability, accessibility and proximity to the edge of Internet, most modern IoT attacks are actualized via attack surface. Even if enterprises deploy IoT services on the intranet, attackers can penetrate through fragile edge routers.

Additionally, the vulnerabilities of an IoT business system like cloud platform vulnerability and big data system vulnerability will give rise to illegal attacks on the system. Generally, many components are designed in the IoT business system like operating system, database, middleware and WEB application. These programs' vulnerabilities or design defects easily cause unauthorized access, data leakage, remote control, and other consequences.[3]

(4) Cybersecurity at the Service-Management Layer

Unlike technological risks at other layers, cybersecurity at the service-management layer mainly lies in people and organizations. Trust and privacy constitute the most basic issues at the IoT service-management layer. Trust ordinarily involves two dimensions, i.e. the trust between interactive entities and a user´s trust in the system. The reliability of IoT devices rests with device components, including hardware (e.g. processor, internal memory, sensor and actuator), software resources, hardware-based software, operating system, driver and application, and power pack. Privacy is the second major problem of IoT devices and services. Entities are interconnected, and data are communicated and exchanged via Internet, which makes a user´s privacy a sensitive topic in many researches.

1. Unit 42, 2020 Unit 42 IoT Threat Report Key findings on how to reduce IoT risks, [2020.6.10].https://start.paloaltonetworks.com/unit-42-iot-threat-report.
2. Wu Gang. “New Opportunities to the Automation Industry in the Era of Internet of Things.” [J] Techniques of Automation and Applications, 2011, 30 (01): 1-9.
3. China Academy of Information and Communications Technology (CAICT). White Paper on Internet of Things (2018). [R\OL]. [2018-09-15]. http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020180919390470911802.pdf.

3. Main Factors That Influence IoT Security

In recent years, hundreds of millions of devices have got access to IoT, and the scale of the IoT industry has continuously expanded. Coupled with the impact of COVID-19, external and internal cyberattacks on IoT have continually increased. Thereinto, the main influencing factors and attack types concerning IoT security cover 10 aspects.

(1) Vulnerabilities

Vulnerabilities are weaknesses in a system or system design that allow intruders to execute commands, access unauthorized data, and (or) launch DDoS attacks. Vulnerabilities can be discovered in all fields of an IoT system, be it vulnerabilities in system hardware or software, or vulnerabilities in policies and processes used in the system and vulnerabilities of system users themselves. Presently, vulnerabilities of IoT security have extended from early business logic vulnerabilities to basic core architecture like hardware architecture, communication protocol, operating system and open-source components. The vulnerabilities in Wi-Fi chips exposed in 2020 affected more than one billion devices, including smartphones, panel computers, laptops, router and IoT gadgets.[1]

(2) Exposure

Ordinarily, IoT devices are deployed in an open environment, and most IoT devices are controlled by people. Anyone can physically access them, and man-made physical attacks are easily launched. It is usually impossible to place IoT devices in protected areas, which is theorized as the ontological security problem of IoT devices. Attackers can affect the normal operation of marking devices by interfering with the sensor ontology. For instance, the power sector plays an important part in national economic development. In the process of long-distance electricity transmission, numerous substation devices can be remotely controlled via IoT. Near unmanned substations, attackers can illegally use infrared devices to interfere with sensors on these devices. If attackers alter key parameters of the devices, the consequences will be unimaginable.[2]

(3) Encryption

Limited by power consumption, computing resources, network bandwidth and other requirements of IoT devices, complex cryptographic algorithms and security protocols cannot be carried. Authentication, key agreement and data confidentiality and integrity protection in communications seem complicated, and the protection of cybersecurity proves difficult. Particularly, the lack of encryption is one of the most common problems in protecting IoT data. Owing to the lack of encryption, threat actors can intercept the network of devices and obtain sensitive data through man-in-the-middle attacks or other eavesdropping methods.

An industrial report in 2015 unmasked some worrying results by scrutinizing manufacturers' devices like TVs, IP cameras, door locks and home alarms. 70% of the devices used unencrypted network services[3], which meant that large numbers of IoT user data would be exposed publicly

1. Mishaal Rahman. New Kr00K vulnerability affects devices with Broadcom and Cypress Wi-Fi chips [EB/OL]. [2020-2-27]. https://www.xda-developers.com/kr00k-wifi-vulnerability-broadcom-cypress/.
2. Wu Tong. "Brief Analysis on IoT Security." [J] Network Security Technology & Application, 2010 (08): 7-8+27.
3. HP News - HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack[EB/OL]. [2014-7-29]. https://www.hp.com/us-en/hp-news/press-release.html?id=1744676#.YmzZpOdByUk.

with only one network configuration error. Besides, according to the survey of Zscaler´s ThreatLabz security research team, by December 2020, 76% of IoT devices were plain text traffic, only 24% of which were encrypted communications.[1]

(4) Distributed Denial of Service Attack (DDoS Attack)

Most DDoS attacks occur at the connection between security and the core network at the perception layer. IoT nodes are large in number, whose presence is in the form of clusters. Therefore, the data-transmission requirement of a great quantity of nodes will incur network congestion and DDoS attacks during data transmission.[2] Now, the scale of IoT device-based botnet continues to expand. Representative IoT DDoS botnet families in 2013 included Linux-based cross-platform DDoS botnet families like CCTV series, ChiekenMM series, BillGates, Mayday, PNScan and gafgyt.[3]

(5) Firmware Hijacking

In case that IoT firmware is not updated timely and a regular updating mechanism is absent, severe cyberattack risks emerge. Devices may seem safe at first. Yet, once new security vulnerabilities or problems are noticed, the devices will be vulnerable to attacks. If these vulnerabilities and problems are not repaired or solved by regular updating, the devices will be attacked. Furthermore, some old devices cannot provide any security updating, and most new devices cannot ensure the timely installation of security patches. Satori, malware that broke out in December 2018, typified firmware hijacking. Satori spread through known vulnerabilities targeted at certain types of IoT devices. It transmitted a worm virus to hundreds of thousands of home routers infected by a remote code execution vulnerability that existed for two years.

(6) Unsafe Interface

The main function of IoT devices is to communicate and process data. These devices are generally equipped with applications, services and protocols for user control. Many manufacturers lump WEB, cloud, API and mobile interfaces to enhance communications. Some serious IoT vulnerabilities often develop from unsafe interfaces. Common problems include the lack of adequate device authorization and identity authentication, as well as the absence of appropriate encryption. Malicious actors often use unsafe interfaces to gain unauthorized access to devices via theft attacks.

(7) Malware

Due to the lack of built-in security function like other devices, IoT devices easily fall into the target of malware. SonicWall´s Global Cyberattack Trends declared that malware attacks against IoT devices increased by 66% in 2020, from 34.3 million times in 2019 to around 56.9 million

1. ZSCALER. Zscaler Study Confirms IoT Devices are a Major Source of Security Compromise, Reinforces Need for Zero Trust Security[EB/OL]. [2021-07-15].
https://www.globenewswire.com/news-release/2021/07/15/2263500/0/en/Zscaler-Study-Confirms-IoT-Devices-are-a-Major-Source-of-Security-Compromise-Reinforces-Need-for-Zero-Trust-Security.html.
2. Zhang Lin, Tao Bo and Li Jiuying. “Research on IoT Technology and Security.” [J] Modern Industrial Economy and Informationization, 2014, 4 (22): 84-85+97.
3. Alibaba Clouder. IoT Botnet and DDoS Attacks Analysis from CERT[EB/OL]. [2018-7-27].
https://www.alibabacloud.com/blog/cert-analysis-on-iot-botnet-and-ddos-attacks_593859.

times in 2020. To be specific, ransomware attacks surged by 62%, from 187.9 million in 2019 to 304.6 million in 2020. Cryptojacking attacks increased by 28% year on year, from 64.1 million in 2019 to 81.9 million in 2021.[1] Hackers used IoT malware to launch brutal attacks, scan open ports or deploy DDoS attacks.

(8) Eavesdropping

Eavesdropping usually occurs by listening to digital or analog voice communication or by eavesdropping and sniffing data. Most IoT components communicate through wireless networks. The wireless channel features openness and lacks security-guarantee nodes, which are vulnerable in form. The wireless signals transmitted among devices tend to be illegally eavesdropped on, interfered and screened. In the environment of sensor network and wireless network, malware has infinite access. Once the intrusion is successful, it will be very easy to spread wantonly. Its concealment, transmissibility and destruction will be more difficult to prevent than TCP/IP network. For example, network worms that do not depend on parasitic files will be extremely difficult to detect and remove in such an environment.[2]

(9) Advanced Persistent Threat

An advanced persistent threat (APT) is a major security issue for various organizations. An APT attack is a targeted cyberattack, in which intruders can illegally access the network and remain undetected for a long time. Attackers aim to monitor network activities and use an APT attack to steal key data. An APT attack is difficult to prevent, detect or mitigate. With the emergence of IoT, massive key data can be easily transmitted among multiple devices. Meanwhile, cybercriminals target at these IoT devices to obtain access to personal or corporate networks, via which they can steal confidential information.

(10) Password Security

IoT device manufacturers set default passwords when selling products. Users often ignore some basic security measures like changing the default passwords. The unintentional carelessness allows malicious actors to access devices by using brute force. Under such circumstances, hackers will submit many passwords or passphrases to find the correct passwords, thus accessing IoT devices, typified by Mirai malware. By logging in with a form containing 61 common default passwords and user names, Mirai malware infects various IoT devices (e.g. routers, cameras, and DVRs). It successfully creates a huge botnet, with more than 400,000 connected devices infected.

In IoT devices, information security can hardly be guaranteed. Therefore, on the one hand, all participants in IoT, including software developers, device manufacturers and data-analysis corporations, should respect the protection of consumers' personal information and fully inform data subjects of how their personal information will be processed. On the other hand, consumers are

1. HI-TECH. IoT malware attacks worldwide surge by 66%[EB/OL]. [2021-04-06]. http://www.securitysa.com/12891r.
2. Peng Yong, Xie Fengjie, Guo Xiaojing, Song Dan and Li Jian. "Research on IoT Security Problems and Countermeasures." [J] Netinfo Security, 2011 (10): 4-6.

advised to strengthen self-protection when using IoT devices. For example, they can set complex and secure passwords for IoT devices, disconnect with the network and cover the camera when IoT devices are not in use, update software timely and read the privacy policies of IoT devices in detail.

Chapter 2

Overview of Global IoT Security Governance

IoT security is a multi-dimensional problem that requires multi-level efforts. On the National Level, it´s a governance problem that needs the development and implementation of IoT security policies, regulations and standards. On the Market Level, enterprises need to work on security solutions in order to protect IoT products and system. Moreover, due to the transnational feature of IoT, international cooperation is needed to achieve the global certification and solution recognized by different countries.

1.National Level: Top-Down Policy Layout for IoT Security

In 2016, the DDoS attack on Dyn resulted in widespread outages across Dyn´s systems, leaving various internet platforms temporarily unavailable to users throughout North America and Europe. Consequently, Dyn faced substantial business interruption issues, recovery costs and reputational damages from the attack. This accident enhanced the governments' attention to IoT security. Countries highlighted the importance of IoT security from economic security and even national security perspectives and tried to set up mechanisms to ensure its resilience. Response system including norms, laws and regulations, and executive orders have been gradually formulated and developed.

(1) The United States

The Mirai Incident in 2016 alerted Washington to pay more attention to IoT security and accelerated the development of laws and standards in relevant fields. Mainly, the United States have made three efforts:

- Establish a trust framework for the IoT ecosystem through strategic principles;
- Protect the security of federal government networks and their critical infrastructure with executive orders and legislation;
- Utilize the NIST´s abilities in standards and guidelines, set a baseline on IoT devices' cybersecurity capability development, and guide departments to integrate IoT security into overall security deployment.

In 2016, the U.S. Department of Homeland Security (DHS) released "Strategic Principles for

Securing the Internet of Things" [1] (The Strategic Principles), which states that IoT security is now a matter of homeland security. The security risks of the IoT will continuously increase because of the complexity of the IoT supply chain and the lack of comprehensive, widely-adopted international norms and standards for IoT security. Therefore, it is necessary to incentivize IoT developers, manufacturers, and users, together with governmental actors, to improve IoT security collectively. This document further settled strategic principles for IoT security to strengthen the trust framework, including Incorporate Security at the Design Phase， Advance Security Updates and Vulnerability Management, Building on Proven Security Practices, Prioritize Security Measures According to Potential Impact, Promote Transparency across IoT, and, Connect Carefully and Deliberately.

In 2017, President Trump issued Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." [2] It indicates that the United States needs to strengthen resilience against Botnets and other automated, distributed threats. Considering that products should be safe at every stage of the life cycle, it is recommended that measures be taken to improve the resilience of the entire Internet ecosystem. Increase transparency of software components and security awareness of the IoT.

Resilience Against Botnets and Other Automated, Distributed Threats. The Secretary of Commerce and the Secretary of Homeland Security shall jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets).

DHS worked closely with the Department of Commerce to lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the Internet and Communications Ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks.

The report, Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats, summarizes the opportunities and challenges in reducing the botnet threat, and offers supporting actions to be taken by both the Government and private sector in order to reduce the threat of automated, distributed attacks. The report is centered around six principal themes:

- Automated, distributed attacks are a global problem.
- Effective tools exist but are not widely used.
- Products should be secured during all stages of the lifecycle.
- Awareness and education are needed.
- Market incentives should be more effectively aligned.
- Automated, distributed attacks are an ecosystem-wide challenge.

1. U.S. Department of Homeland Security. Strategic Principles for Securing the Internet of Things（IoT）[EB/OL]. (2016-11-15) [2022-03-10] .https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf
2. Presidential Executive Order 13800. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure Support to Critical Infrastructure [EB/OL]. (2017-05-11) [2022-03-10] https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

Created with broad input from stakeholders and experts, the report lists five complementary goals that would improve the resilience of the Internet ecosystem. The recommended actions include ongoing activities that should be continued or expanded, as well as new initiatives, such as an effort to increase software component transparency and a public campaign to support awareness of IoT security.

The United States Senate has introduced the “Internet of Things Cybersecurity Improvement Act 2017” and “Internet of Things Cybersecurity Improvement Act 2019” (referred to as the S.1691 Act). These Acts require that IoT devices applied to the Federal Government must at least meet the minimum-security standards to address their related cyber risks. After several amendments, the first National IoT security law, “Internet of Things Cybersecurity Improvement Act of 2020”[1] (hereinafter referred to as “the Act”) finally became public law.

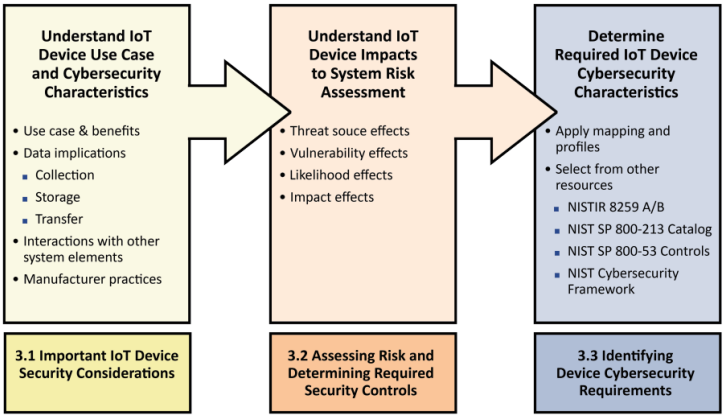
“The Act” requires the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) to take specific steps to improve the cybersecurity of IoT. NIST provides standards and guidelines for the federal government to use the IoT devices, establishes and publishes minimum cybersecurity standards related to such devices, and establishes guidelines on security vulnerabilities that agencies, contractors, and subcontractors follow in common. Federal purchases of IoT devices must meet the minimum cybersecurity standards issued by NIST, and OMB is responsible for reviewing government policies to ensure they meet NIST standards and guidelines.

In May 2020, the technical report of NISTIR8259A "IoT Device Cybersecurity Capability Core Baseline" [2] was released to provide the minimum standard for the cybersecurity capability of IoT devices and to help users understand the six aspects of the IoT devices, which are related to their common characteristics and basic principles of the cybersecurity capability. First, device identification. IoT devices can be uniquely identified logically and physically; Second, device configuration. The configuration of the IoT device´s software can be changed, and such changes can be performed by authorized entities only; Third, data protection. The IoT device can protect the data it stores and transmits from unauthorized access and modification; Fourth, logical access to interfaces. The IoT device can restrict logical access to its local and network interfaces and the protocols and services used by those interfaces to authorized entities only; Fifth, software update. The IoT device’s software can be updated by authorized entities only using a secure and configurable mechanism; Sixth, cybersecurity State awareness. The IoT device can report on its cybersecurity state and only make that information accessible to authorized entities.

In November 2021, an IoT standard of SP800-213, “IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements,” [3]was published by NIST. It is developed to help organizations incorporate IoT devices as system elements into exist-

1. U.S. Congress. Internet of Things Cybersecurity Improvement Act of 2020 [EB/OL].(2020-12-04) [2022-03-10]. https://www.congress.gov-/116/plaws/publ207/PLAW-116publ207.pdf
2. NIST. IoT Device Cybersecurity Capability Core Baseline [EB/OL].(2020-05-29) [2022-03-10].https://doi.org/10.6028/NIST.IR.8259A
3. NIST. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements [EB/OL]. (2021-11-29) [2022-03-10]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213.pdf

ing information systems from a risk management perspective. The publication also provides guidelines on how to identify the cybersecurity requirements of IoT devices and how to understand the risk management of IoT. It helps organizations determine the impact of IoT devices on the system and organizational security capabilities and provides effective system control and management of risks.



Source: NIST SP800-213 "IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements"

(2) EU

In addition to stringent regulatory requirements on enterprise data protection obligations in GDPR, the EU has developed several guidelines on IoT security construction:

- Protect the security of IoT in critical information infrastructure. Improve the security awareness and ability by setting the security baseline.
- Protect the software development security and emphasize the core baseline throughout the life cycle of IoT products and services.
- Ensure the security of the IoT supply chain; all parties in the supply chain should make effective security decisions according to the guidelines.

In November 2017, the European Union Agency for Cybersecurity (ENISA) released the guidance of "Baseline Security Recommendations for Internet of Things in the context of critical information infrastructures." With the analysis of IoT architecture, threat and risk, as well as the security gap, it provides a security baseline, which is based on six vertical applications of IoT, namely: smart homes, smart cities and smart public transportations, smart grids, smart cars, smart airports, eHealth and smart hospitals.

Meanwhile, the guide makes seven suggestions to promote the healthy and rapid development of the European IoT in critical information infrastructure areas:

- Promote harmonization of IoT security initiatives and regulations
- Raise awareness for the need for IoT cybersecurity
- Define secure software/hardware development lifecycle guidelines for IoT
- Achieve consensus for interoperability across the IoT ecosystem

- Foster economic and administrative incentives for IoT security
- Establishment of secure IoT product/service lifecycle management
- Clarify liability among IoT stakeholders

In November 2019, ENISA released the report of "Good Practices for IoT-Secure Software Development Lifecycle Security." [1]This study presents good practices for IoT security, with special attention to software development security in IoT products and services. The study recommends following the principles of the Software Development Life Cycle (SDLC) for Security to run through the requirements, software design, development/implementation, testing and acceptance, integration and deployment, maintenance, and disposal cycles with a security baseline. The study underlines the need to consider end-to-end IoT security, not only to focus on smart devices, network protocols, and communications but also taking a step back and methodically integrating cybersecurity by design principles throughout the software development lifecycle.

In November 2020, ENISA released "Guidelines for Securing the Internet of Things"[2] (hereinafter referred to as the "Guidelines"), which set out guidelines to ensure the security of the supply chain of IoT. Guide IoT manufacturers, developers, integrators, and all stakeholders involved in the supply chain of IoT to make security decisions in all aspects of the life cycle of IoT, such as construction, deployment, and evaluation. The guide makes the following suggestions for building the security of IoT:

- Forging better relationships between actors
- Cybersecurity expertise should be further cultivated
- Security by design
- Take a comprehensive and explicit approach to security
- Leverage existing standards and good practices

（3）Australia

With the rapid development of the IoT market, Australia finds it necessary to improve the overall cybersecurity for market-orientation IoT devices to develop a trustworthy market for consumers and minimize the economic and national security risks. In practice, the Australian government has issued guidelines to enhance the security of IoT devices, which also provides a secure basis for the development of consumer IoT.

In September 2020, the Australian Government issued the "Code of Practice：Securing the Internet of Things for Consumers" [3] (from now on, referred to as the "Practice Guidelines"). The Australian government wants to use this as the first step to improve the security of devices on IoT and enhance consumer confidence in the technology. The "Practice Guidelines" sets out 13 principles:

1. ENISA. Good Practices for Security of IoT-Secure Software Development Lifecycle [EB/OL] (2019-11-19) [2022-03-10]. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
2. ENISA. Guidelines for Securing the Internet of Things [EB/OL]. (2020-11-09) [2022-03-10]. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things
3. Australian Government. Code of Practice：Securing the Internet of Things for Consumers [EB/OL].(2020-09-03) [2022-03-10]. https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

- No duplicated default or weak passwords
- Implement a vulnerability disclosure policy
- Keep software securely updated
- Securely store credentials
- Ensure that personal data is protected
- Minimize exposed attack surfaces
- Ensure communication security
- Ensure software integrity
- Make systems resilient to outages
- Monitor system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data

The Australian Government recommends industry prioritize the top three principles because action on default passwords, vulnerability disclosure, and security updates will bring the most significant security benefits in the short term.

（4）The UK

The UK government believes that consumer IoT products that offend the cybersecurity baseline can intrude on privacy or even personal safety. At the same time, malicious cyberattacks against IoT can pose economic risks. Therefore, in addition to industry self-regulation, the UK is enacting legislation to strengthen regulation of consumer IoT products, promote market transparency and ensure that consumer IoT products sold in the UK meet basic security requirements.

In February 2020, the UK updated "Consultation on the Government´s Regulatory Proposals Regarding Consumer Internet of Things（IoT）Security" [1](hereinafter referred to as the "Consultation") to identify consumer IoT devices that meet the security baseline requirements with security labels. These devices include but are not limited to： connected children's toys and baby monitors, connected safety-related products such as smoke detectors and door locks, Smart cameras, TVs and speakers, wearable health trackers, connected home automation and alarm systems, and connected appliances (e.g., washing machines, fridges), Smart home assistants. The Consultation considers mandatory requirements for consumer IoT products sold in the UK to meet the following three requirements: First, IoT device passwords must be unique and not resettable to any universal factory setting; Second, Manufacturers of IoT devices need to provide a public point of contact as part of a vulnerability disclosure policy to make sure security researchers and others can report problems; Third, Manufacturers of IoT devices need to explain the minimum cycle of security updates explicitly. The Consultation also plans to create a labeling scheme to help consumers choose trusted IoT products.

1. U.K. Department for Digital, Culture, Media and Sport .Consultation on the Government's Regulatory Proposals Regarding Consumer Internet of Things（IoT）Security [EB/OL].(2020-02-03) [2022-03-10]. https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security

In December 2021, the UK introduced the "Product Security and Telecommunication Infrastructure Bill" [1] (PSTI Act) to protect citizens, networks, and infrastructure from unsafe Internet consumer products. The PSTI Act explicitly prohibits the use of default passwords, specifies the minimum period of security updates, and provides contact points for vulnerability reporting. Regulators have the authority to impose a penalty of up to £ 10 million or 4% of their global turnover on companies that do not comply with regulations. A penalty of up to £ 20,000 per day may be imposed for continued violations.

(5) Canada

Canada attaches great importance to protecting personal information in IoT applications. Devices manufactured and developed by equipment manufacturers must comply with relevant legal personal information and privacy requirements. The Canadian government also hopes consumers can recognize and manage the privacy-related functions in the devices and enhance their privacy protection awareness and ability.

In August 2020, the Office of the Privacy Commissioner of Canada (OPC) published "Privacy guidance for manufacturers of Internet of Things Devices" [2](hereinafter referred to as the "guidance"). The guidance requires IoT device manufacturers to comply with the "Personal Information Protection and Electronic Documents Act" (PIPEDA) and develop IoT devices that respect privacy and comply with privacy laws. IoT device manufacturers should follow the guidelines to protect privacy if their products can collect personal information, such as lights, doorbells, locks, smoke detectors, alarms, televisions, cameras, electrical appliances, toys, watches, or health trackers, etc. At the same time, consumers should also have privacy protection awareness and specific capabilities when they enjoy the convenience brought by smart devices. The guidance provides consumers with knowledge about identifying and mitigating risks, such as checking how personal information will be used or shared and turning off device networking when it is not in use.

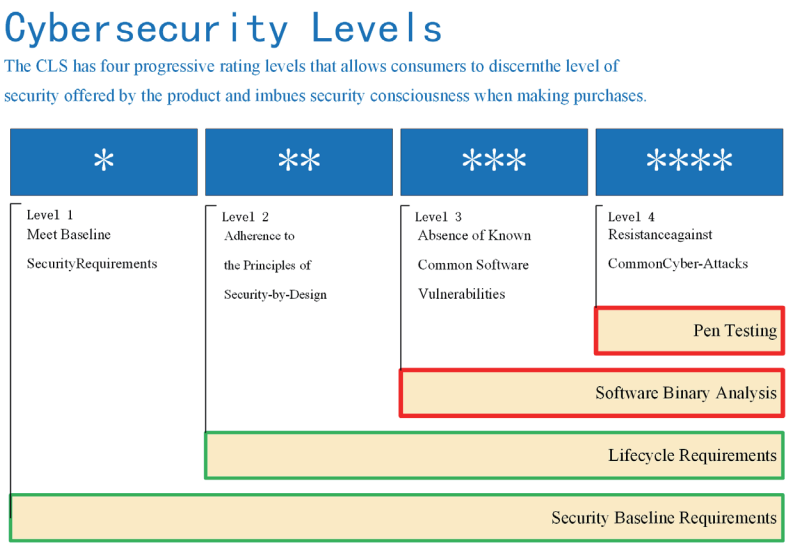
(6) Singapore

Singapore is the first country in the Asia-Pacific region to introduce the Cybersecurity Labeling Scheme to strengthen the security management of IoT products. IoT enterprises can prove that their products can meet the basic and general safety standards by submitting relevant certificates; if it is necessary to prove that the product has a higher level of safety protection, the manufacturer needs to apply for the evaluation report of the designated laboratory. Label grading enables consumers to identify products with a higher level of cybersecurity, thus promoting the development of the IoT industry in a safer direction.

In November 2020, Singapore introduced the Cybersecurity Labelling Scheme (CLS) for customers' smart devices to improve the security level of IoT and enhance cyberspace security. CLS is the first label program in Asia-Pacific. Smart devices are rated according to the level of cybersecurity regulations, and IoT device manufacturers can apply to join the program voluntarily. In Octo-

1. U.K. Department for Digital, Culture, Media and Sport .Product Security and Telecommunication Infrastructure Bill [EB/OL].(2021-12-24) [2022-03-10]. https://bills.parliament.uk/bills/3069
2. The Office of the Privacy Commissioner of Canada. Privacy guidance for manufacturers of Internet of Things Devices [EB/OL].(2020-08-20) [2022-03-10].https://www.priv.gc.ca/en/privacy-topics/technology/gd_iot_man/

ber 2021, the “Cybersecurity Certification Guide” [1]was released with four levels of certification: Security Baseline Requirements, Lifecycle requirements, Software Binary Analysis, and Pen Testing. These four levels increase in turn, reflecting the product's increased resistance to possible cyberattacks.



Source: Singapore CSA 2021 “Cybersecurity Certification Guide”

(7) Mexico

In particular, Mexico focus on the protection of personal information on IoT. In July 2017, National Institute for Access to Information and Data Protection[2](INAI) issued recommendations on the use of IoT devices. It is suggested that the personal information collected, stored, processed, and transmitted by IoT may include sensitive information such as health status and biometric data. Without security standards for IoT device manufacturers, it´s challenging to protect the personal information of consumers in IoT. Therefore, all participants in IoT, such as software developers, equipment manufacturers, and data analysis companies, should devote attention and efforts to protecting consumers’ personal information and clearly explain how these data are being processed; On the other hand, consumers are recommended to strengthen self-protection abilities. For example, create complex and secure passwords, disconnect the internet, cover the camera when devices are not in use, update the software in time, and read the privacy policy of devices carefully.

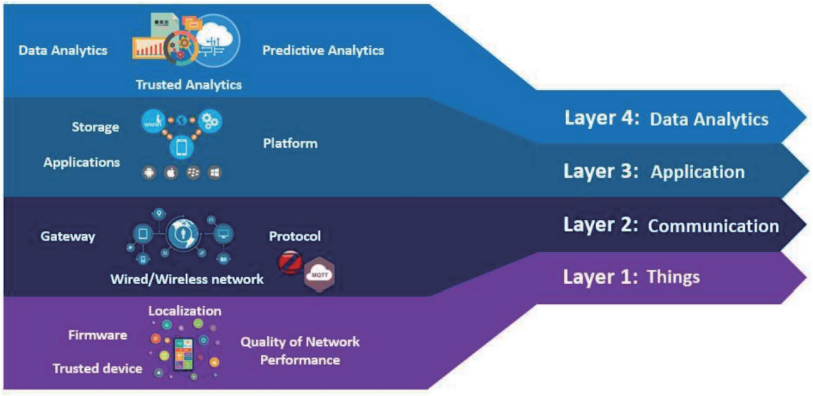
(8) Malaysia

Malaysia systematically analyzed the IoT system and then lay stress on collectively building IoT security ecology. In May 2020, Malaysia issued “Guidelines for Secure Internet of Things”[3]

1.Singapore. Cybersecurity Certification Centre. Cybersecurity Certification Guide[EB/OL].(2021-10-6) [2022-03-10]. https://www.csa.gov.sg/-cls
2.Mexico National Institute for Access to Information and Data Protection. EMITE INAI RECOMENDACIONES PARA USO DE DISPOSITIVOS CON TECNOLOGÍAS DEL INTERNET DE LAS COSAS [EB/OL] (2017-07).[2022-03-10].http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-226-17.pdf
3. Malaysia. Guidelines for Secure Internet of Things[EB/OL]. (2020-05-05) [2022-03-10].https://www.cybersecurity.my/data/content_-files/56/2074.pdf

(hereinafter referred to as the “Guidelines” in this section). It suggests that IoT devices' needs and privacy for IoT are required to ensure the proper confidentiality, integrity, authentication, and access control, among others. The “Guidelines” put forward the IoT security framework, analyze the main threats and vulnerabilities faced by IoT, and put forward security controls for the IoT system. It requires that the three core participants in the IoT system, manufacturers, providers, and consumers, can understand IoT’s security and build a reliable and safe IoT system in common.

IoT security framework



Source: Malaysia,2020, “Guidelines for Secure Internet of Things”

(9) China

IoT has been widely used in various industries in China. Its application and development promote economic development and the procedure of social informatization, as well as the reform of the industrial structure and the progress of digital governance. China has accelerated the construction of IoT security systems from the top-level design, laws, regulations, and standard formulation. It aims to promote the healthy and orderly development of IoT effectively.

In February 2013, “Guiding Opinions of the State Council on Promoting the Orderly and Healthy Development of the Internet of Things” (hereinafter referred to as the "Guiding" in this section)[1] was released and enhanced that ensuring IoT security is the essential prerequisite to making the IoT Industry more competitive in the world market. Thus, it´s necessary to strengthen security awareness and pay attention to information system security and data protection. Moreover, the core application field of IoT further requires an increased the abilities of a security evaluation, risk assessment, and security protection. The “Guiding” also emphasized main tasks, including: strengthening protection and management abilities to ensure cybersecurity; improving the level of cybersecurity management and data protection of the IoT; accelerating the research and development of cybersecurity technology; promoting the construction of cybersecurity system; establishing and improving the supervision, inspection, and security evaluation mechanism; effectively ensuring the security and trustworthy of data collection, transmission, processing and application in IoT.

1. Guiding opinions of the state council on promoting the orderly and healthy development of the Internet of Things [EB/OL].(2013-02-17) [2022-03-10].http://www.gov.cn/zwgk/2013-02/17/content_2333141.htm

In 2017, "The 13th Five-Year Plan for the Development of Internet of Things (2016-2020)" [1] was issued by the Ministry of Industry and Information Technology (MIIT). The Five-Year Plan gives explicit directions for the industries to strengthen security, including: making important breakthroughs in the research and development of core security technologies and specially-used security products; basically establishing IoT security mechanisms such as security evaluation, risk assessment, security precaution, and emergency response, and enhance the security capacities of IoT infrastructure, critical systems, and important information.

In 2019, the MIIT issued "Guiding Opinions on Strengthening Industrial Internet Security," and proposed the main tasks of building an industrial cybersecurity management system, improving the security protection standard, and strengthening the ability of data security protection.

In 2021, MIIT, CAC, the Ministry of Science and Technology etc. departments jointly issued "Three-year Action Plan for the Construction of New Infrastructure for the Internet of Things (2021-2023)"[2]. The Action Plan sets basic principles, including: balancing development and security; improving the autonomy and controllable of core technologies; strengthening the security protection capacity; enhancing the flexibility of the industrial supply chain; increasing data security protection; and improving the safe and reliable abilities, effectively preventing and resolving potential security risks.

In terms of laws and regulations, "Cybersecurity Law of the People's Republic of China," "Data Security Law of the People's Republic of China," "Personal Information Protection Law of the People's Republic of China," "Regulation on Protecting the Security of Critical Information Infrastructure," and "Measures for Cybersecurity Review (2021)" etc. are issued and implemented to provide the legal basis for the security supervision of IoT industry.

In terms of standards, different levels of specific IoT standards are developed in recent years. First, general security standards incorporate IoT as a category of objects or applications. The national standard of GB/T 22239-2019 "Information security technology—Baseline for classified protection of cybersecurity" etc. extend IoT requirements for classified protection. Meanwhile, similar measures are also applied to the general security standards of risk assessment, security monitoring, notification and warning, data protection, and emergency treatment.

Secondly, specific technical standards of IoT have been developed. On the national standardization level, the National Information Security Standardization Technical Committee (TC260) has formulated a series of IoT security standards.

In October 2021, MIIT issued "Guidelines for the Construction of the Internet of Things in Basic Security Standard System (Version 2021)" [3], which further points out the standard´s important role in regulation security-guarantee. In March 2022, MIIT issued "Guidelines for the Con-

1.MIIT. The 13th Five-Year Plan for the Development of Internet of Things (2016-2020) [EB/OL]. (2017-01-19)[2022-03-10]. http://www.e-gov.org.cn/article-164273.html

2. Ministry of Industry and Information Technology, Central Committee of Cybersecurity and Informatization, etc. Three-year Action Plan for the Construction of New Internet of Things Infrastructure (2021-2023) [EB/OL]. (2021-09-27)[2022-03-10].

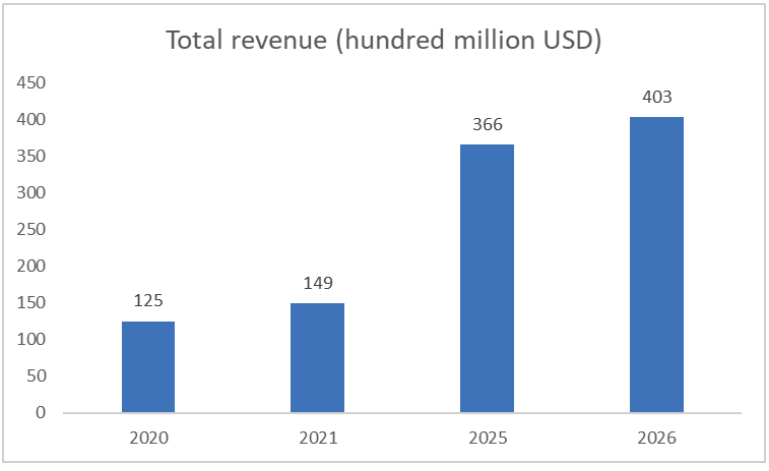
3. MIIT. Guidelines for the Construction of the Internet of Things in Basic Security Standard System (Version 2021) [EB/OL]. (2021-10-25) [2022-03-10]. https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2021/art_d78e9d282eb44709998705d3214b668c.html

struction of Internet of Vehicles in Cyber Security and Data Security Standard System" [1], which requires building a relatively comprehensive systemic standard for cyber security and data security on the Internet of Vehicles by the end of 2025. It also requires improving the service capabilities, upgrading the standard application level, and supporting the safe and healthy development of the automobile networking industry.

GB/T 37044—2018	Information security technology—Security reference model and generic requirements for Internet of things
GB/T 36951—2018	Information security technology—Security technical requirements for application of sensing terminals in the internet of things
GB/T 37024—2018	Information security technology—security technical requirements of gateway in sensing layer of the internet of things
GB/T 37025—2018	Information security technology—Security technical requirements of data transmission for the internet of things
GB/T 37093—2018	Information security technology—Security requirements for IoT sensing layer access to communication network

2. Market Level

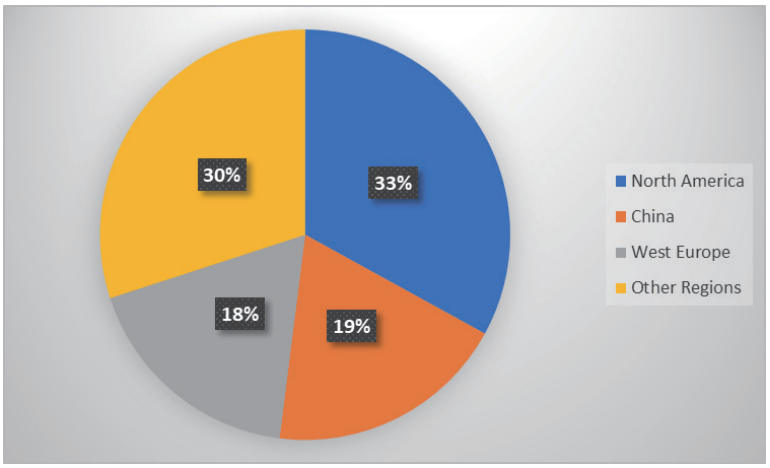
The trend of IoT development advances a stable market for IoT security services. Based on the *Research Report "IoT Security Market by Type, Component*, *Solution*, *Service*, *Application Area and Region" published by Markets and Markets,* the global IoT security market value is about $12.5 billion in 2020 and $14.9 billion in 2021. This data will surge to $36.6 billion in 2025 and $40.3 billion in 2026, at a Compound Annual Growth Rate (CAGR) of 22.1%. [1]



Source: Markets and Markets Research Report "IoT Security Market by Type, Component, Solution, Service, Application Area and Region"

1. Markets and Markets. IoT Security Market by Type, Component, Solution, Service, Application Area, and Region-Global Forecast to 2025.https://www.marketresearch.com/MarketsandMarkets-v3719/IoT-Security-Type-Network-Cloud-13451509/; IoT Security Market by Type, Component, Solution, Service, Application Area, and Region-Global Forecast to 2026.https://www.marketsandmarkets.com/Market-Reports/iot-security-market-67064836.html

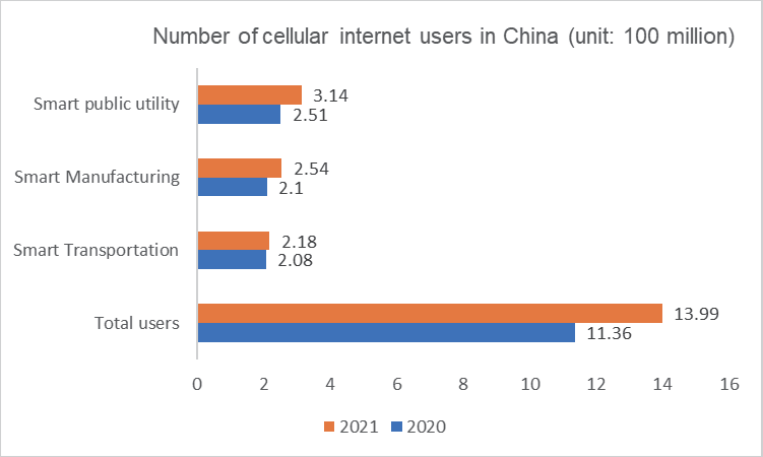
According to another report published by Gartner[1], from the industrial perspective, the IoT security market covers three areas, including the manufacturing and natural resources industry, consumer automobile industry, and transportation industry. From a regional perspective, North America, China, and Western Europe rank among the top three in the global IoT security market.



Source: Gartner, "Forecast: Enterprise and Automotive IoT Edge Device Security, Worldwide, 2019-2025"

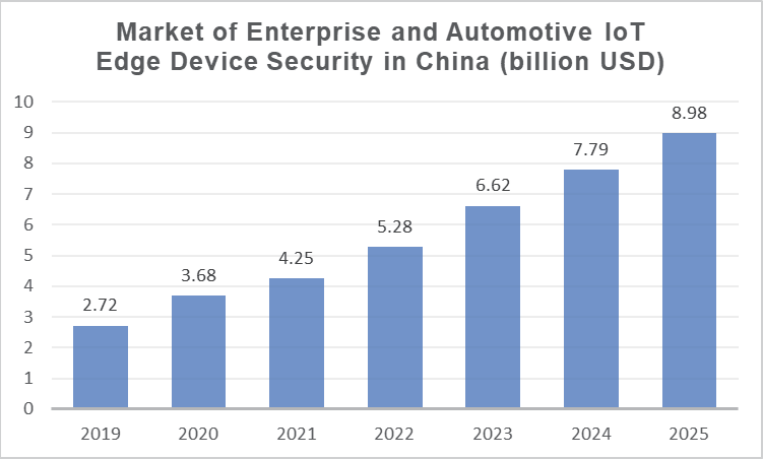
China's IoT market expand continuously in recent years, with a considerable increase in the total number of IoT connections. However, referring to the core application fields, the proportion of smart public utilities and intelligent manufacturing in 2021 almost keeps equal to previous years, and the proportion of intelligent transportation decreased slightly. According to "Statistical Report of the Telecommunications Industry in 2020" [2] and "Statistical Report of the Telecommunication Industry in 2021" [3] published by MIIT, there are 1.136 billion Chinese cellular IoT users in 2020. By the end of 2021, there are 1.399 billion cellular IoT users, increasing 23% compared to the number in 2020. Futhermore, the number of IoT terminals applied in smart public utilities reached 314 million, accounting for 22.4% (251 million in 2020, accounting for 22.1%); 254 million in intelligent manufacturing, accounting for 18.2% (210 million in 2020, accounting for 18.5%); 218 million in intelligent transportation, accounting for 15.6% (208 million in 2020, accounting for 18.3%).

1.Gartner, Forecast: Enterprise and Automotive IoT Edge Device Security, Worldwide, 2019-2025
2. MIIT. Statistical Report of the Telecommunications Industry in 2020 [EB/OL]. (2021-01-22) [2022-03-10].https://www.miit.gov.cn/gxsj/tjfx-/txy/art/2021/art_057a331667154aaaa6767018dfd79a4f.html
3. MIIT. Statistical Report of the Telecommunications Industry in 2021 [EB/OL]. (2022-01-25) [2022-03-10]. https://www.miit.gov.cn/gxsj/t-jfx/txy/art/2022/art_e2c784268cc74ba0bb19d9d7eeb398bc.html



Source: MIIT. "Statistical Data of the Telecommunications Industry in 2020 and 2021"

With the upgrading of China's communication network infrastructure, the reforming of traditional industries, and the acceleration of the cloud platform construction, data is increasingly valued as a newborn resource. All these contributed to the enrichment of China´s IoT ecosystem. According to the data from Gartner[1], the market value of China's enterprise and automotive IoT edge devices reached USD 368 million (about RMB 2.323 billion) in 2020 and is expected to reach USD 425 million (about RMB 2.683 billion) in 2021 and is expected to reach USD 898 million (about RMB 5.669 billion) in 2025.



Source: Gartner, "Forecast: Enterprise and Automotive IoT Edge Device Security, Worldwide, 2019-2025"

In general, though IoT and IoT security markets have not seen significant growth under COVID-19 challenge, it is not easy to maintain stability and show a growth trend. With the diffi-

1. Gartner, Forecast: Enterprise and Automotive IoT Edge Device Security, Worldwide, 2019-2025 (2021-05-17) [2022-03-10]. https://www.gartner.com/en/documents/4001635

cult recovery of the global economy, the continuous improvement of infrastructure, the optimization and innovation of IoT technology, and the urgent need for digital transformation in various countries, the prospect of IoT and IoT security market are still optimistic.

3. International-Organization Level

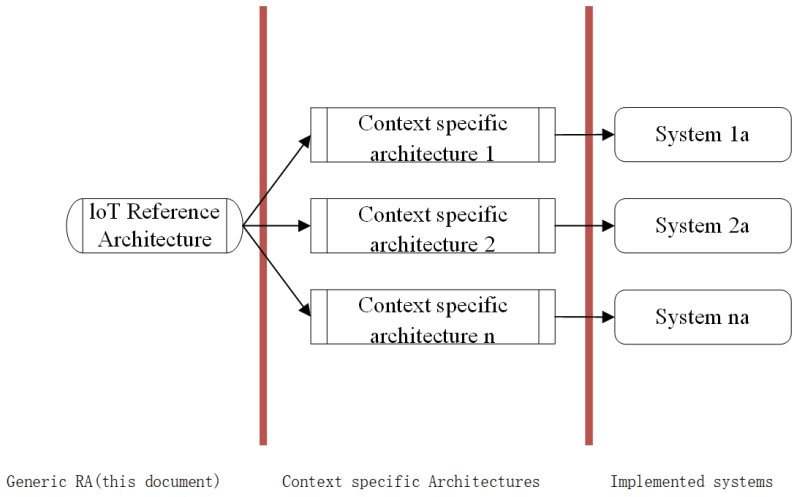
International organizations attach great importance to the development of IoT. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), International Telecommunications Union (ITU), and the Internet of Things Security Alliance (ioXt) have successively issued relevant standards, regulations, and security principles to promote the development of the IoT security system, to improve the security of critical components, to apply security norms to emerging fields, and to advocate the industry to follow the security principles collectively. These procedures can enhance the public confidence in IoT applications, and give full scope to the value of IoT in the digital era.

(1) ISO

The framework for IoT security standards is developed by ISO to promote its healthy and efficient development; Second, stress the importance of the basic framework and provide standardized guidance for the extensive technical foundation of IoT; Third, focus on privacy protection and promote the security and credibility of IoT.

In 2018, ISO/IEC 30141 “Internet of Thing (IoT) - Reference Architecture” is published, including a general IoT Reference architecture in terms of defining system characteristics, a Conceptual Model, a Reference Model, and architecture views (functional view, system view, networking view, and usage view) for IoT. The standard provides the overall guidance of the architecture and reference model for implementing the global IoT industry. It has made significant contributions in promoting the rapid and healthy development of the global IoT industry.

Figure 1 - From generic Reference Architecture to context specific architecture



Source: ISO/IEC 30141:2018 Internet of Things(IoT)-Reference Architecture

Sensor network is one of the core technologies used in IoT. The ISO/IEC 19637, "Information technology-Sensor network testing framework," [1]published in 2016, is an important basic standard in sensor networks. The standard defines a testing framework for sensor networks and solves the problem of protocol testing compliance for heterogeneous sensor networks. Testing agents in the test framework can provide differentiated support services according to sensor network specifications. Standard guidance creates test platforms for testing other sensor network protocols.

Biometrics authentication technologies based on physiological or behavioral features (such as fingerprint, face, voiceprint) are being applied in the field of IoT security. However, the fragmentation of networking environments for mobile devices brings a risk to mobile device certification using biometric technology. ISO/IEC 27553 "Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices" (draft) points out the security challenges and threats, and designs a security framework for using biometric technology for authentication on mobile devices. It also provides high-level security requirements for authentication from functional components to mobile applications. At the same time, IoT security and privacy protection standard, ISO/IEC 27400 "Cybersecurity-IoT security and privacy" is also being developed in progress.

(2) ITU

The contributions of ITU international standard on IoT security can be concluded into three aspects. First, ITU also focuses on the security framework and devotes to standardizing standard requirements, and promotes the cryptographic technology to support the security and industrial development of IoT. Second, it emphasizes privacy protection and standardize personal information used in the IoT. Third, it supports IoT security applications in industry and smart city as well as internet of vehicle security and focus on automatic response in case of emergency.

ITU has put forward a series of security standards for IoT, including ITU-T Y.2066 "Common requirements of the Internet of things," ITU-T Y.2068" Functional framework and capabilities of the Internet of things," ITU-T Y.4103 "Common requirements for Internet of things (IoT) applications," ITU-T X.1361, "Security framework for the Internet of things based on the gateway model," etc. These documents put forward common requirements for IoT and its applications and functional and security frameworks. Additionally, ITU-T X.1362 "Simple encryption procedure for Internet of things (IoT) environments" is intended to support IoT security with cryptographic technology and help the development of IoT.

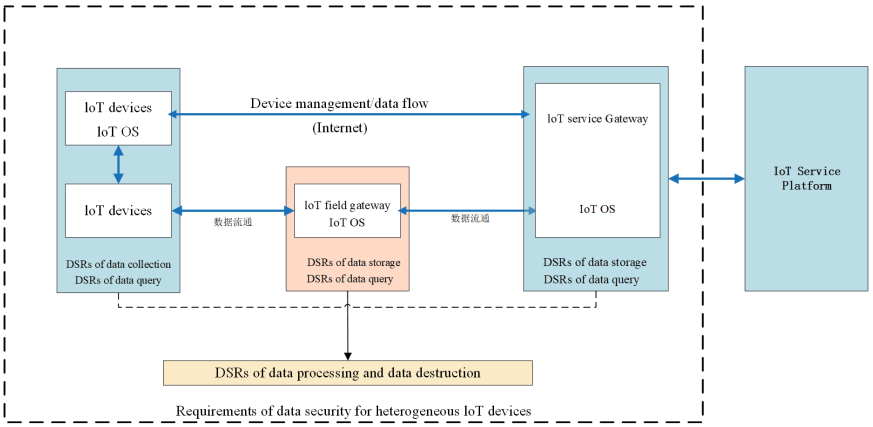
ITU-T X.1363 "Technical framework of personally identifiable information handling system in the Internet of things environment" [2] informs users of the appropriate principles of service operators' collecting and controlling data. Users can manage personal data, including personal identity information, in the IoT ecosystem according to their intentions. For example, given the principle

1. ISO/IEC 19637:2016 Information technology- Sensor network testing framework. (2016-12) [2022-03-10]. https://www.iso.org/standard/65695.html.
2. ITU-T X.1363. Technical framework of personally identifiable information handling system in Internet of things environment. (2020-05) [2022-03-10] https://www.itu.int/rec/T-REC-X.1363-202005-P

that only with the authorization can the personal data be collected and stored, users have the right to check the history of data sharing between service providers. Standards, just then, can provide a technical framework for processing personally identifiable information in an IoT among multiple service providers.

In November 2021, ITU-T Y.4810 “Global information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities” [1]focused on the data security of IoT devices in smart city scenarios. A data security threat and demand model was designed for mass heterogeneous IoT devices. The corresponding technical standards for data protection are also put forward.

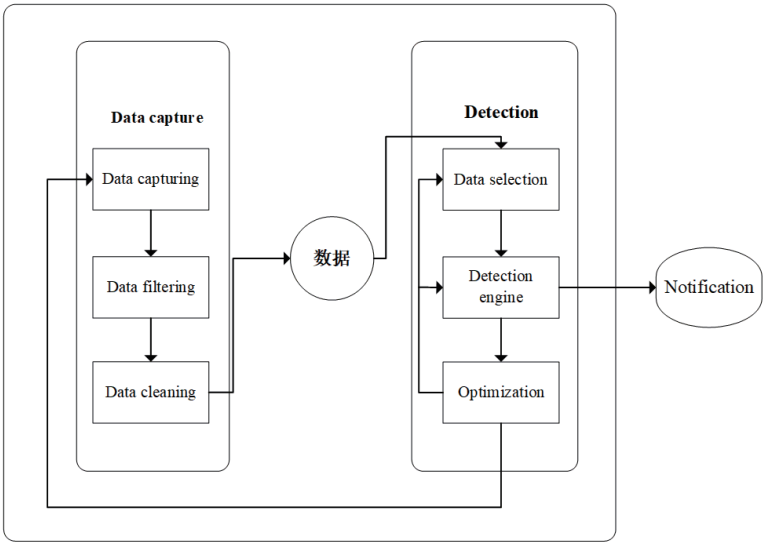
This Recommendation specifies requirements for data security of heterogeneous Internet of things (IoT) devices, including, under specific scenarios, a data security threat (DST) and requirement model.



Source: ITU-T Y.4810 “Global information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities.”

As for the internet of vehicles, ITU-Y.4119 “Requirements and capability framework for IoT-based automotive emergency response system” sets the standards and requirements for emergency detection equipment and emergency response centers. ITU-T X.1373 "Secure software update capability for intelligent transportation system communication devices" pays attention to the update of connected vehicle security software to repair errors, improve performance and avoid accidents. ITU-T X1376“Security-related misbehavior detection mechanism using big data for connected vehicles” is the first international standard to use big data analysis for cybersecurity of Intelligent Transportation Systems. It establishes a mechanism from two dimensions of data collection and detection to detect possible improper behavior by designers and security solution providers.

1. ITU-T Y.4810.Global information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities. (2021-11) [2022-03-10] https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.4810-202111-I!!PDF-E&type=items



Source: ITU-T X1376 "Security-related misbehavior detection mechanism using big data for connected vehicles."

(3) UN

The global connected vehicle market in 2021 is about $23.6 billion and is expected to reach $56.3 billion by 2026, with an annual growth rate of 19%.[1] The cybersecurity of connected cars must be placed in a critical position to provide a safe basis for the prosperity and development of the market. The United Nations has promulgated three milestone vehicle laws and regulations to strengthen connected vehicle security governance to achieve this goal.

On January 22, 2021, United Nations Regulation 155, "Uniform provisions concerning the approval of vehicles regarding cyber security and cyber security management system," entered into force. It is the first international regulation on vehicle network security. In addition to Regulation 155, Regulation 156 "Software update and software update management system" and Regulation 157 "Automated Lane Keeping Systems (ALKS)" are released by the UN and these standards constitute a landmark international rule focusing on intellective connected vehicles and are applicable to the 54 parties in 1958 Agreement.

The Regulation 155 specifies that cybersecurity protects road vehicles and their functions from cyber threats, and Cyber Security Management System (CSMS) defines a systematic risk-based approach defining organizational processes, responsibilities, and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks. Manufacturers need to meet three requirements to apply for international approval marks. First, they must carry out a cyber security risk assessment, test against cyber security attacks, and implement appropriate security measures in vehicle type design. Second, they must implement supply chain management and

1. Markets and Markets. Connected Car Devices Market worth 57.15 Billion USD by 2021. (2021-01-22) [2022-03-10].https://www.marketsandmarkets.com/PressReleases/connected-cars.asp

prove that risks related to suppliers are identified and managed through the cyber security management system. Third, it is necessary to monitor and report continuously, such as assessing whether the implemented cyber security measures are still valid in the face of new threats discovered. Continually monitor and analyze vehicle-related cyber threats, vulnerabilities, and attacks to provide data evidence capabilities while respecting privacy.

The cyber threat against the intelligent connected vehicle may affect the safe operation of the vehicle or stop some functions. The software may be modified to involve the relevant performance, data integrity, confidentiality, and availability, resulting in losses. Therefore, the Regulation 155 lists different cyber threat attacks faced by vehicles in the annex and puts forward relevant solutions from the two dimensions of the vehicle itself and outside. For example, if a cyber-attack destroys or blocks the information transmission between vehicles, recovery measures such as detection and anti-denial of service attack should be taken; If there is an attack on the back-end server, which makes it unable to interact with the vehicle and provide services for the vehicle, it is necessary to strengthen the security control of the back-end system. In case of system interruption, there are relevant service recovery schemes.

Regulation 156, "Software update and software update management system," is the first international regulation to manage software updates for Over-The-Air Technology (OTA) of vehicles. Regulation 157, "Automated Lane Keeping Systems (ALKS)," is the first international law to cover the SAE Level 3 system. The purpose of the Regulation is to establish uniform provisions for the Automated Lane Keeping Systems (ALKS) to provide security for SAE Level 3 auto-driving.

(4) ioXt

ioXt (Internet of secure things) Internet of Things Security Alliance, composed of leading technology and product manufacturers, is the fastest growing and industry-oriented security certification organization for IoT. It is committed to enhancing the transparency and adoption of security in IoT devices, enhancing the trust of producers, sellers, and consumers in IoT, and removing security barriers to the popularization and development of IoT.

Google, Amazon, and Meta have all contributed to ioXt´s current security standards enabling the highest level of security available for applications and devices, including cameras, smart speakers, mobile phones, smart lights and switches, network controllers, etc. As ioXt adds additional security standards we attract the top companies from each product sector.

The certification program of ioXt is increasing the importance of IoT security in all countries and promoting the promulgation of relevant laws and regulations. In December 2020, "Internet of Things Cybersecurity Improvement Act" in the United States, which was also jointly promulgated by the IoXt-represented Security Ecology Alliance of the IoT and the National Institute of Standards and Technology (NIST).

ioXt's Security Principles:

ioXt–proposed eight security principles, authorizing certified laboratories to evaluate IoT devices and quantify their security level. These eight principles relate to product safety, upgradability, and consumer transparency:

Principle 1–No Universal Passwords

Often, high-volume consumer devices are all shipped with the same default password. Typically, users want to quickly deploy their new device, so many do not take the simple step of changing the default password to a new one. Shipping each new device with a unique factory-programmed password is a simple first step in making it more difficult for adversaries to gain access to or take control of, potentially, hundreds of deployed devices.

Principle 2–Secured Interfaces

Any microcontroller-based device has a multitude of interfaces and ports that can be accessed either locally or remotely. The primary application will use some of these ports during operation and for communications. However, the rest–particularly any that function as external communication interfaces must be secured. Likewise, any IC-to-IC interfaces—such as between the microcontroller and a display controller—must be secured. It is recommended that all interfaces be encrypted and authenticated during use.

Principle 3–Proven Cryptography

In a world of open and interoperable technologies, the use of industry-recognized, open, and proven cryptographic standards is essential. The use of closed, proprietary cryptographic algorithms is not recommended. The use of open cryptographic standards encourages participation by all developers, engineers, and stakeholders to be continually evaluated for potential vulnerabilities against new security threats.

Principle 4–Security by Default

It is essential that when a consumer purchases a new device, it is already set for the highest possible levels of security. Shipping a product with no or minimal security options configured can pave the way for adversaries to take advantage. The consumer out-of-box security experience should be that all possible security measures are enabled. Developers should not leave a consumer unprotected by default.

Principle 5–Signed Software Updates

With the increasing number of consumer smart-home devices that can update themselves automatically over the air being shipped, the priority is that every update should be signed cryptographically. In this way, hackers are prevented from attempting to update a device with malicious code.

Principle 6–Software Updates Applied Automatically

Consumers shouldn't have to become administrators of their own devices, faced with deciding whether to update a product's software image. If an update needs to be made, it should be deployed and implemented automatically. Moreover, updates should be applied at times when they will not compromise the device's operation. For example, a smart-connected washing machine should not be updated while the machine is in use.

Principle 7–Vulnerability Reporting Scheme

Often, consumers who experience a problem with their embedded smart-home device are unsure who to contact. Has it been compromised? Is there a new vulnerability that should be reported? This principle pledges that product manufacturers will create a means for customers to

report problems and communicate their concerns regarding product security.

Principle 8–Security Expiration Date

As with product warranties, which have an expiration date after purchase, the period during which security updates are available should also be defined and communicated to the consumer. Continuing to support a product with security updates involves continued engineering costs, so consumers need to make informed decisions at the time of purchase. Manufacturers also have the option to offer extended warranties to offset ongoing security updates.

The ioXt Smart Cert tag can be obtained from products certified by the ioXt test. At present, more and more participants are participating in the ioXt federation, and the scope of product categories for compliance certification is expanding. On April 15, 2020, ioXt announced an expanded compliance program to unify consumer electronic safety standards. [1]This plan is defined and established by multiple network operators, major consumer electronics companies, chip suppliers, and test labs. Enhance the security transparency of IoT through multi-party collaboration, and verify the security compliance of devices in IoT by third-party test labs, enabling consumers to identify products based on ioXt security principles and security hardware platforms and protocols. On April 15, 2021, the ioXt Compliance Program added test certification for VPN applications and new mobile applications, extending security compliance to mobile application platforms.

(5) The PSA Certified 10 Security Goals

PSA Certified is a global partnership providing a security framework and independent evaluation that demonstrate your commitment to security best practice and alignment to worldwide regulations. PSA Certified builds on the foundations of the Platform Security Architecture (PSA), which was created to address the need for scalability and consistency across large-scale IoT deployments. PSA Certified can be used by the entire ecosystem, no matter your job title.

PSA Certified can be thought of as providing the recipe (architecture documents) and ingredients (open source code, threat models, development boards, and models) to make security easier, no matter your level of security expertise. Through this approach, we are working with the electronics industry to make the development of trustworthy chips, firmware, software, and devices more straightforward, giving the ecosystem the confidence to create.

PSA Certified is committed to creating a foundation of trust for all connected devices and making this as easy as possible to prevent these simple IoT attacks from taking place. To achieve this, the Platform Security Model document, containing 10 goals, was devised to guide security best practices and provide a practical checklist to follow.

PSA Certified takes a holistic view of security, considering both hardware and software security. The 10 security goals are in the DNA of PSA Certified and inform the whole security framework and evaluation scheme.

1. IoXt.ioXt Alliance Expands Security Compliance Program[EB/OL]. (2020-04-15)[2022-03-10].https://www.ioxtalliance.org/news-events-blog/ioxt-alliance-expands-security-compliance-program

Every product has unique functional and security requirements however, these goals outline the common requirements that should be implemented into every connected device. The 10 security goals guide security design by covering the security foundations, allowing products and features to be developed on top while also providing a set of requirements the ecosystem can rely on. The PSA Certified 10 Security Goals:

● Unique Identification

To interact with a particular device, a unique identity should be assigned to the device and this identity should be attestable. This identity facilitates trusted interaction with the device, for example, exchanging data and managing the device.

● Security lifecycle

Devices should support security lifecycle that depends upon software versions, run-time status, hardware configuration, status of debug ports, and the product lifecycle phase. Each security state of the security lifecycle should be attestable and may impact access to the device

● Attestation

Attestation is evidence of the device´s properties, including the identity and lifecycle security state of the device. The device identification and attestation data should be part of a device verification process using a trusted third party.

● Secure boot

To ensure only authorized software can be executed on a device, secure boot and secure loading processes are required. Unauthorized boot code should be detected and prevented. If the software cannot compromise the device, unauthorized software may be allowed.

● Secure update

Secure updates are required to provide security or feature updates to devices. Only authentic and legitimate firmware should be updated on the device. Authentication, at the time of download, may be performed however, the execution of the update must be authorized via the secure boot.

● Anti-rollback

Preventing rollback to previous software versions is essential to ensure that previous versions of the code can´t be reinstated. Rollback should be possible for recovery purposes only when authorized.

● Isolation

Isolation aims to prevent one service from compromising other services. This is done by isolating trusted services from one another, from less trusted services and un-trusted services.

● Interaction

Devices should support interaction over isolation boundaries to enable the isolated services to be functional. The interfaces must not allow the system to be compromised. It may be required to keep the data confidential. Interaction should be considered both within the device and between the device and the outside world.

● Secure storage

To prevent private data being cloned or revealed outside the trusted service or device, it must

be uniquely bound to them. Confidentiality and integrity of private data is typically achieved using keys, which themselves need to be bound to the device and service.

● Cryptographic/trusted services

A minimal set of trusted services and cryptographic operations should be implemented as the building blocks of a trusted device. These should support critical functions including security life-cycle, isolation, secure storage, attestation, secure boot, secure loading and binding of data.

Chapter 3

Main Challenges to IoT Corporate Compliance

Boosted by the development of the digital economy, the global IoT industry has developed rapidly into a new stage of IoE (Internet of Everything). This not only injects new impetus to global economic development, but also poses new security risks. As a result, security incidents occur frequently, with increasingly severe impacts. In particular, due to the blurry policy on cybersecurity and complex technological application, as well as the tension between outdated policy and new technological applications, IoT enterprises encounter many challenges in terms of policy and technological compliance, which increases their operating costs and has a negative impact on global operation and overall development of the IoT industry.

1. Increasingly Stringent Cybersecurity Policy and Blurry Legal Boundary

Against the backdrop of frequent IoT security incidents and increasingly negative impacts, China, the United States, Europe, and other countries attach more attention to IoT security, personal privacy protection and data-security protection, and promulgate and implement cybersecurity policies including laws, regulations and guidelines in the above fields, aiming to establish a flexible and stable IoT system to ensure domestic economic security and national security. Since cybersecurity policies in various countries stay in the early stage of exploration and formulation, and most relevant laws and regulations belong to upper-level legislation that plays the role of strategic layout, specific implementation provisions remain absent, resulting in the blurry state of cybersecurity policies in various countries.

(1) Major cybersecurity incidents of IoT continue to increase, and IoT security develops from voluntary compliance to a mandatory requirement.

First, major cybersecurity incidents in IoT continually emerge. In May 2021, the Colonial Pipeline, located in Alabama Pelham, became the victim of a cyber attack , which caused Colonial Pipeline to lose control over most of its oil pipelines. For security reasons, Colonial Pipeline urgently blacked out all pipeline transportation businesses. As Colonial Pipeline took charge of 45% of fuel supply on the east coast of the United States, fuel supply became insufficient for a

time, and the oil price in the United States rose. Apparently, the wide range of attacks and a great influence on IoT enterprises expose the weaknesses of relevant national and corporate networks. This spurs various countries around the world to seriously examine their network-defense measures, accelerate the upgrading of national network-defense systems at the technological level (e.g. the deployment of multi-factor identity authentication, encryption, endpoint detection and other technological means), and quicken the transfer of federal government-information systems to the cloud.

Second, IoT security develops from voluntary compliance to mandatory requirements. In May 2019, the Department for Digital, Culture, Media and Sport (DCMS) of the United Kingdom released The Consultation on the Government's Regulatory Proposals Regarding Consumer Internet of Things (IoT) Security, which promoted the enforcement of the top three guidelines for security measures and required retailers to sell consumer IoT products only with security labels.[1]

In December 2020, the United States issued the Internet of Things Cybersecurity Improvement Act, requiring the National Institute of Standards and Technology (NIST) to publish federal government standards and guidelines for the use of IoT devices and all the federal agencies to ensure that all the IoT contractors meet the minimum standards set by NIST by December 2022. Director of the Office of Management and Budget would achieve the binding force of NIST standards by controlling procurement, which required all the IoT contractors that would undertake federal government's contracts at all levels to meet compliance requirements.

In January 2019, Japan adopted *The Amendment to the National Institute of Information and Communications Technology (NICT) Law,* which amended the general legal provision *Prohibition of Unauthorized Computer Access* and allowed penetration testing of IoT-device security without notifying enterprises and citizens.[2]

Third, as a trend, various countries face more policy-related challenges in optimizing regulatory rules. In the long run, with the long-term development of the IoT industry, Europe and the United States are obliged to further improve regulatory regulations related to IoT security and optimize regulatory rules. Simultaneously, the UK, China, Russia and other developing countries underline the legislation of IoT security and strengthen the regulation of IoT enterprises. The legislative regulation of various governments in the field of IoT security serves as an important prerequisite for promoting the sound development of the IoT industry. Irrefutably, however, regulatory policies promulgated by various countries will mean more policy-related challenges to IoT enterprises. Enterprises certainly have to face more problems on policy compliance and technological compliance, in which IoT enterprises bear more social responsibilities and compliance costs.

1. Zhang Xiye. "Trends of IoT-Security Legislation in the United States and the Inspiration to China." [J] China Internet, 2021 (06): 32-37.
2. Zhang Xiye. "Trends of IoT-Security Legislation in the United States and the Inspiration to China." [J] China Internet, 2021 (06): 32-37.

Table 1 Cybersecurity Policies Promulgated by the United States, European Union and China

The United States	U.S. Department of Homeland Security (DHS)	*Strategic Principles for Securing the Internet of Things (IoT)*
	United States Congress	*Internet of Things Cybersecurity Improvement Act*
	United States Congress	*Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*
	Presidential Executive Order	*Securing the Information and Communications Technology and Services Supply Chain*
	State of Washington	*Data Breach Notification Laws*
	State of California	*The Security of Connected Devices*
	State of California	*California Consumer Protection Act (CCPA)*
	State of California	*California Privacy Rights Act (CPRA)*
	Presidential Executive Order	*Executive Order on America's Supply Chains*
	Presidential Executive Order	*Executive Order on Improving the Nation's Cybersecurity*
	United States Congress	*United States Innovation and Competition Act of 2021* (Partially involving supply chain security)
The European Union	European Parliament and Council of the European Union	*General Data Protection Regulation (GDPR)*
	European Parliament and Council of the European Union	*Data Governance Act (DGA)*
	European Union Agency for Cybersecurity (ENISA)	*Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures*
	European Union Agency for Cybersecurity (ENISA)	*2020 Guidelines for Securing the Internet of Things*
	European Union Agency for Cybersecurity (ENISA)	*Guideline on Incident Reporting*
	European Data Protection Board	*Guidelines on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR*
	European Data Protection Board	*Guidelines on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications*
China	Office of the Central Cyberspace Affairs Commission	*Measures on Security Assessment of Overseas Use of Data (Draft for Comments)*
	Office of the Central Cyberspace Affairs Commission	*Regulations on the Administration of Network Data Security (Draft for Comments)*
	Standing Committee of the National People's Congress	*Data Security Law of the People's Republic of China*
	Standing Committee of the National People's Congress	*Personal Information Protection Law*
	Standing Committee of the National People's Congress	*Cybersecurity Law*
	Standardization Administration of the People's Republic of China	*Technological Requirements for Internet of Things Data Transmission Security in Information Security Technology*
	Standardization Administration of the People's Republic of China	*Typical Model and General Requirement for Information Security Technology in Internet of Things Security*

(2) Legislation on personal privacy and data security becomes stringent, and corporate compliance cost rises.

Obviously, the laws and regulations on IoT security promulgated by various countries raise higher security requirements for IoT enterprises. On the basis of analyzing IoT security demand, risk and threat, IoT enterprises are required to comprehensively sort out security demands of IoT

systems from the angles of user and business, grade security risks (destruction and tendency), and take countermeasures to cope with IoT security risks. Therefore, IoT enterprises have to meet higher technological requirements, such as taking security as overall evaluative standards in the design stage and promoting the improvement of their product-security updating, vulnerability management and other security measures.

With regard to personal privacy security, the United States, the European Union and China are accelerating the legislative work of privacy protection. For example, the United States released *California Consumer Protection Act (CCPA)* in 2018, and revised it as *California Privacy Rights Act (CPRA)* in 2020, which emphasized the importance of protecting consumers' personal privacy data and balancing commercial trade and privacy protection.

The EU´s *General Data Protection Regulation (GDPR)* came into force in May 2018. GDPR is viewed as the most stringent data protection law in the history of the European Union. In line with the jurisdictional principles of *Lex Loci* and *Lex Personalis,* enterprises that provide information products or services or monitor users' information in the territory of the European Union need to comply with the privacy protection provisions in *GDPR*.

In August 2021, the Standing Committee of the National People´s Congress adopted the *Personal Information Protection Law*, which explicitly restricted the excessive collection of personal information, the abuse of facial recognition, big data-enabled price discrimination against existing customers and other violations of users' privacy, and raised higher privacy-protection requirements for enterprises.

As required by privacy-protection provisions in various countries, IoT enterprises must well perform their duties in the internal audit of corporate compliance in relation to personal privacy and data protection, and check, update and improve the existing privacy policies in accordance with the requirements of national laws and regulations, so as to ensure their compliance with laws and regulations. In particular, IoT enterprises must ascertain whether they comply with privacy provisions of overseas laws and regulations under special circumstances. In addition, IoT enterprises need to adjust privacy-protection technologies to meet the compliance requirements of "complete deletion" and "access to machine-readable data" in national laws and regulations.

With regard to data protection, national legislative work mainly revolves around transnational data transmission and data-security protection. For example, in 2018, United States Congress passed and enforced *Clarifying Lawful Overseas Use of Data Act (CLOUD Act),* which gave American law enforcement agencies the right to obtain data from communication service providers. In 2019, the State of Washington passed *Data Breach Notification Laws* to further improve data protection mechanisms and require enterprises to take countermeasures immediately after a data breach.

On the basis of the General Data Protection Regulation, the European Union issued A European Strategy for Data in 2020 and the Data Governance Act soon afterward, which emphasized the healthy flow of data in the territory of the European Union to boost the development of the EU digital economy.

China officially passed the *Data Security Law of the People's Republic of China* in 2021[1], which aimed to ensure data security, promote data development and utilization and protect the legitimate rights and interests of individuals and organizations. Office of the Central Cyberspace Affairs Commission also released *Measures on Security Assessment of Overseas Use of Data and Regulations on the Administration of Network Data Security* to optimize cross-border data transmission and security management mechanisms.

Under the regulation of the above laws, IoT enterprises must face the importance of cross-border data transmission and data protection. More significantly, they need to improve their capacities of data protection, regularly monitor vulnerabilities and formulate work plans to ensure the integrity, availability and reliability of data transmission in IoT devices. In case of data leakage, enterprises will be confronted with huge business risks and legal penalties. In order to meet governmental requirements on data compliance, enterprises need to draw up compliance strategies at multiple levels (e.g. analyzing data risks, formulating compliance plans and establishing personal-data protection systems), and construct corporate data-management systems to deal with governmental data-security inspection.

Against such a backdrop, IoT enterprises face more stringent technological requirements in the field of data security and personal privacy. They need to invest additional human and material resources to build technological teams and conduct an internal review of their products to meet the requirements on compliance. Taking data-security compliance as an example, IoT enterprises need to fulfill lifecycle data security management, which involves data collection, data storage, data-security processing, data-preservation strategy, data-security transmission, device-end data security, cross-border data transmission and data-security processing authority management.

For example, in the process of data collection, IoT enterprises need to design products in the light of basic principles of openness and transparency, choice and consent and consistency of rights and responsibilities, and formally start R&D and production processes only after strict risk and compliance assessment by compliance teams. After products are released and applied, technological teams need to irregularly evaluate data protection and impact of products, analyze sensitive data and conduct compliance processing to ensure the legitimacy and compliance of data collection.

With regard to data transmission, in order to ensure the security and effectiveness of data transmission, technological teams need to classify collected data according to the source, content and purpose of data, clarify the sensitivity levels of various data and conduct security processing according to the value, sensitivity, impact and distribution scope of the data. For instance, sensitive information like personal communication content, personal privacy data and biometric data can be desensitized by algorithm, and the data can be transmitted only after the transmission channel and terminal device are securely encrypted, so as to ensure that no security problems arise like data leakage in the transmission.

1. Standing Committee of the 13th National People's Congress. Data Security Law of the People's Republic of China. [EB/OL]. [2021-06-10]. http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.

In addition to complex technological requirements in the above processes, with the rapid development of IoT, the data collected and produced by IoT enterprises in the process of production and operation increase explosively, which will enormously intensify the difficulty and compliance cost of corporate data management.

(3) COVID-19 Breeds Uncertainty in the Formulation of IoT Regulatory Policies in Various Countries.

COVID-19 has directly affected the capacities of national governmental agencies to guide and monitor IoT development. Governments have to centralize primary social resources and attention to cope with the outbreak of COVID-19. Political priority of the research and formulation of IoT security policies must give way to COVID-19.

Under the impact of COVID-19, IoT enterprises have to adjust their operation models, which may give rise to new compliance risks and speed up the invalidation and obsolescence of the existing regulatory policies. For example, with respect to corporate technological application, COVID-19 facilitates the automatic, intelligent and data-based transformation of IoT enterprises and forces IoT enterprises to accelerate the application of AI, big data and wireless communication technologies, so as to reduce the artificial dependence on IoT devices and hedge against the impact of COVID-19 on the normal operation of IoT devices. This significantly advances the automatic transformation of the IoT industry in the short term.

The wide application of automation technology in the short term not only poses new technological compliance risks to IoT enterprises, but also causes new regulatory problems to governmental regulatory policies, which results in potential risks to the compliance of IoT enterprises. In the layout of corporate supply chain, COVID-19 rocks supply-chain security of global IoT enterprises, and compels them to realize the importance of establishing complete supply chain systems. In order to make up for their external dependence, IoT enterprises re-arrange the upstream and downstream supply chains involved in their products, hoping to improve the stability, sustainability and security of their products. On the one hand, the extension of the industrial chain widens the physical boundary and technological scope of enterprises that operate IoT devices. On the other hand, the extension of the industrial chain forces IoT enterprises to face more policy and technological compliance requirements and intensifies the compliance risks of IoT enterprises.

2. Technological Complexity Increases Compliance Costs

Under the regulation of national cybersecurity policies and regulations, IoT enterprises must bear the social responsibility to deal with technological security risks in the future, so as to meet corresponding requirements on compliance. As the IoT system integrates a variety of emerging technologies, tremendous complexity exists no matter in technological application, standard formulation, compatibility or in security-mechanism construction, which incontrovertibly poses challenges to the policy compliance of IoT enterprises. In the future, IoT enterprises must increase compliance investment to deal with security issues like the standardization and compatibility of relevant technologies.

(1) IoT system seems structurally complex, and the security strategy achieves unsatisfactory results.

The connection between IoT devices features a dynamic state and instantaneity[1], and interactive actors in the IoT system embody complexity and diversity, which means great internal and external challenges to cybersecurity governance of IoT.

First, the fragmentation of IoT devices intensifies, making it difficult to form long-term efficacious security solutions. With the industrialization of IoT, hundreds of millions of IoT terminals are widely used in various industries, enterprises and places, with complex use cases, different platforms and varying terminal functions. On the one hand, IoT devices often employ low-energy technologies of slow processors, limited computing capacity and low memory storage, which disenables most IoT devices to support complex security solutions.

On the other hand, the basic systems and communication protocols used among IoT devices differ, and the interconnection and interoperability prove poor. Besides, the main assets of the IoT system commonly consist of system hardware, software, service and data generated by service. Therefore, IoT security requires enterprises to ensure the security of tangible objects like devices and the value of intangible objects like data, information and service. Considering this, the protection of IoT-device security can hardly be realized and long-term efficacious security solutions can hardly be formed.

Second, internal differentiation of the IoT system strengthens, making it difficult to form "end-to-end" security protection. A typical IoT system structurally includes four layers, each of which interconnects via different wireless or wired communication protocols. Ideally, IoT security solutions can achieve "end-to-end" comprehensive security protection. However, the four-layer architecture of IoT involves various industrial-chain links, resulting in diverse participating roles and complex structures. From hardware chips, sensors and wireless modules at the terminal layer, to communication operators at the network layer, and to software development, system integration and platform service at the platform-application layer, all the links can hardly be well coordinated.

Third, in geographical location, IoT is distributed in a scattered way, making it difficult to actualize security protection. IoT is widely applied in places for production and life. Therefore, the locations of terminals are scattered outside, making it more challenging to monitor. Factors like man-made destruction, illegal movement, loss of sensing node or inability to work and users' low willingness to upgrade are common. Consequently, IoT terminals conk out for a long time and tend to be maliciously controlled, making security protection difficult.

Fourth, the understructure of traditional IoT industrial security remains weak, forming a disadvantage for overall security protection. The IoT industry covers a wide range. Not only various emerging industries, but also traditional industries like transportation, medical care, home furnishing and logistics realize transformation and upgrading via IoT. Traditional industries develop later

1. Atzori L, Iera A, Morabito G. "The internet of things: A survey." [J] Computer networks, 2010, 54 (15): 2787-2805.

(2) IoT integrates with new technologies, which increases the difficulty of cybersecurity protection.

Presently, 5G, edge computing, digital twins and other technologies quickly come to rise, and IoT speedily integrates with new technologies, which not only promotes the development of IoT, but also complicates the cybersecurity pattern of IoT.

First, the integration of IPv6 and IoT increases the difficulty of security detection. The development of IPv6-based next-generation Internet provides new ideas for improving the efficiency of cybersecurity governance and innovating cybersecurity mechanisms. The super-large address space of IPv6 protocol owns natural advantages in dealing with some cyberattacks, and improves cybersecurity in traceability, anti-hacker sniffing capacity, routing protocol and end-to-end IPSec secure transmission capacity[1]. However, with the development of mobile Internet, IoT, cloud computing, big data and other technologies, new security problems emerge in the integration process of IPv6 with new technologies and applications.[2]

On the one hand, albeit IPv6 address expansion can solve the shortage of network address, the query of massive addresses proves complex, which increases the difficulty of security detection. On the other hand, transitional protocols will be used from IPv4 to IPv6. Attackers can use the vulnerability of transitional protocols to bypass security monitoring and attack. Therefore, the coexistence of IPv4 and IPv6 causes some security problems. Additionally, terminal security means new challenges to the formulation of IPv6 security strategy and cybersecurity regulation.[3]

Second, the connection between 5G and industrial IoT increases potential attack surface. With the development of 5G technology, various governments advocate and promote the implementation of smart city IoT. The collaborative innovation of IoT terminal and edge security industry ushers in huge development opportunities.[4] The rise of 5G produces both new opportunities and new weaknesses. Particularly, with the connection of industrial IoT and 5G, cybercriminals have strengthened their attacks on industrial IoT devices and key infrastructure. Devices from pumps, temperature monitors, IP cameras or those connected to unmanned aerial vehicles are more vulnerable to a variety of attacks, like spear phishing, credential disclosure, malware or ransomware.

Third, edge computing hardly covers the strategy of security protection. As security risks that arise from centralized, cloud-based data storage enlarge, many enterprises start to deploy and implement edge-based computing (i.e. processing data at the edge of network rather than in a cloud data center). All the data will be leaked if a centralized cloud server is broken. Small data packets stored on multiple edge computing nodes will disseminate the risks, and if one node is broken, it may only affect a small amount of the data. However, the number of edge computing nodes is gigantic, including edge cloud, edge gateway, edge controller, and other edge terminals in various

1. National Administration of State Secrets Protection. “Analysis on Security Risks and Countermeasures of IPv6 Network.” [EB/OL]. [2018-08-14].http://www.gjbmj.gov.cn/n1/2018/0814/c411145-30228506.html.
2. Xu Zhen and Han Yanni. “Analysis on Security Risks and Countermeasures of IPv6 Network.” [J] Confidential Work, 2018 (07): 51-53.DOI:10.19407/j.cnki.cn11-2785/d.2018.07.025.
3. Xu Zhen and Han Yanni. “Analysis on Security Risks and Countermeasures of IPv6 Network.” [J] Confidential Work, 2018 (07): 51-53.DOI:10.19407/j.cnki.cn11-2785/d.2018.07.025.
4. Chen Shenghua. “Discussion on IoT Security in the 5G Era.” [J] Network Security Technology & Application, 2021 (08): 82-84.

forms. The complexity and heterogeneity of terminals intensify and hardly cover the security protection strategy. Coupled with the limited resources and capacity of edge facilities, edge computing nodes cannot effectively provide security capacity in line with the cloud data center. Edge node data is easy to be damaged, and infrastructure software is difficult to be protected. Besides, edge computing adopts open API, open network-function virtualization and other technologies and introduces them openly, which easily exposes edge nodes to external attackers.[1]Sequitur Labs, an IoT security corporation, reported that: "Over the past five years, edge devices have been used as attack vectors to harm networks or systems. Once cybercriminals come into contact with edge devices, they can quickly and easily interrupt operational activities, resulting in downtime, loss of revenue and damage to the reputation of the organization."[2]

(3) IoT supporting technologies diversify, and compliance responsibility and cost remain high.

First, the technological environment of the IoT system is becoming more complex. The IoT system integrates various technologies like sensing, communication, storage and computing. When enterprises apply any kind of new technology, they need to bear corresponding compliance responsibility and cost. Specifically, IoT is an open-Internet-architecture-based huge system that comprises digital facilities with sensing and application functions and interconnects with data communication via network protocols, formed by a variety of technologies and devices.[3] Therefore, safe, stable and efficient IoT is inseparable from the strong support of cloud computing, algorithm, communication, AI and other technologies. And the diversity of IoT-system-support technology undoubtedly increases the costs and risks of enterprises when they apply technologies. Taking cloud computing technology in IoT system as an example, in order to ensure that cloud computing technology used in their products and services meets compliance requirements, enterprises need to establish internal monitoring, audit and governance mechanisms in the processes of cloud-data transmission, storage, backup, retrieval and access, and designate special personnel for internal compliance verification to ensure the security and compliance in data transmission. In addition to internal review, enterprises need to regularly accept the compliance audit investigation of third-party institutions on data encryption, system and data access control, service protocol, etc. Simultaneously, enterprises need to formulate emergency plans in advance and forge corresponding risk-response mechanisms according to security levels required by laws or regulations, so as to deal with corresponding risks caused by violations of external cloud computing suppliers. In the future, as the IoT system continuously develops, the technological environment of the IoT system becomes more complex, with more emerging technologies applied into the IoT system. Correspondingly, IoT enterprises will face more security risks and pay more technological costs.

Second, the diversity of technological standards increases the costs of corporate compliance.

1. China Academy of Information and Communications Technology (CAICT). White Paper on Internet of Things (2020). [EB/OL]. [2020-12-10]. http://www.caict.ac.cn/kxyj/qwfb/bps/202012/P020201215379753410419.pdf.
2. Nitin Dahad. Edge IoT devices will provide easier entry point for cyberattacks in 2022– Embedded.com [EB/OL]. [2021-12-24]. https://www.embedded.com/edge-iot-devices-will-provide-easier-entry-point-for-cyberattacks-in-2022/
3. Čolaković A, Hadžialić M. "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues" [J] Computer networks, 2018, 144: 17-39.

The standardization of IoT architecture and related technologies provides an important support for the future development of the IoT system; therefore, the IoT system is advised to be established in a flexible, safe, open and systematic network architecture, so as to realize the integration of various technologies and diverse sensing devices in the IoT system and support the overall interconnection of IoT. Admittedly, many international standardization organizations, alliances, academia, and industries are making efforts to develop and innovate IoT standardization. For example, ITU, ETSI, IETF, IEEE, W3C, OneM2M, OASIS and NIST have formulated standards for IoT security architecture, IoT network security, IoT device security and encryption and system security.[1]Yet, comprehensive network architecture and technological standards that can solve technological diversity and device heterogeneity have not been established. IoT enterprises have to face complex security terms and technical standards to meet the compliance requirements of governmental laws and regulations.

Table 2 Industrial Standards and Provisions in Relation to the Compliance of IoT Enterprises[2]

Provisions	Types or Names	Content
Industrial Standards	**ISO/IEC 27001**	ISO/IEC 27001 is an international standard for information security management system (ISMS), which provides best practical guidance for various organizations to establish and operate information security management systems.
	ISO/IEC 27017	ISO/IEC 27017 provides guidance for information security of cloud computing. It is recommended to implement information security control targeted at cloud, which is a supplement to ISO/IEC 27001 Standard.
	CSA STAR	STAR cloud security assessment is new and unique service that aims to deal with specific issues related to cloud security. It is an enhanced version of ISO/IEC 27001.
	ISO 9001	ISO 9001 is transformed from the first quality management system standard BS 5750 (written by BSI) in the world. It is a relatively mature quality framework in the world so far. It mainly focuses on the products or services provided by enterprises. It is a systematic guiding program and normative framework to ensure the product quality and operation of enterprises.

1. China Academy of Information and Communications Technology (CAICT). White Paper on Internet of Things (2020). [EB/OL]. [2020-12-10]. http://www.caict.ac.cn/kxyj/qwfb/bps/202012/P020201215379753410419.pdf.
2. Collected and Re-organized from the Internet.

Industrial Standards	**AICPA SOC2 Type II**	SOC2 TypeII is an authoritative certification in the field of data security, which is used to ensure that service providers can safely manage data and protect the interests of enterprises and the privacy of their customers.
	ETSI EN 303645	ETSI EN 303645 is security technological standard for consumer electronics IoT products released by the European Union. It mainly stipulates cybersecurity of consumer IoT products and related services, and includes some commercial IoT products. It aims to establish a security defense line for consumer IoT products and protect user privacy. Presently, IoT laws are promoted in the UK, which are also based on technological requirements of the Standard.
	ioXt Alliance Certification	ioXt Alliance Certification is the only authoritative industry-leading IoT security certification program in the world. ioXt Alliance is jointly initiated by technology and equipment manufacturing giants such as Google, Amazon, T-Mobile and Comcast.
Governmental Regulations	**EU, *General Data Protection Regulation* (GDPR)**	EU's *General Data Protection Regulation (GDPR)* aims to protect basic privacy and personal information security of data subjects in the EU and the European Economic Area. It raises more stringent protection standards and requirements, and sets high default costs, which enormously improves the security, compliance standards and costs of enterprises in the information processing and protection of EU citizens.
	State of California, *California Consumer Protection Act (CCPA)*	*California Consumer Protection Act (CCPA)* officially came into force on January 1, 2020. It aims to strengthen the protection of consumers' privacy and data security. *CCPA* is regarded as the most stringent privacy legislation in the United States.[1]
	The United States, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*	*CLOUD Act* breaks through traditional data storage-address models, extends the law-enforcement effectiveness of the United States to the world, and establishes a cross-border data-acquisition system centered on the United States, which has a great impact on corporate compliance and data sovereignty.

Third, IoT enterprises are forced to improve compatibility and expansibility under compliance regulations. Under the regulation of national laws and regulations, IoT enterprises must make technological adjustments to their products and services in R&D, testing and application, so as to solve

1. Qin Lijuan. "A Comparative Study on the Legislation and Application of 'Right to Be Forgotten' in EU and the United States." [D] Nanjing Normal University, 2019.

technological problems of compatibility and expansibility in IoT. First of all, IoT enterprises need to solve the compatibility of IoT connections and realize the interoperability of heterogeneous devices at the software and hardware levels. Due to the lack of relevant standards and specifications in the early stage of IoT development, major software service providers and hardware manufacturers adopt their own technological interface standards, resulting in great heterogeneity in the existing technological environment of IoT. The existing IoT architecture does not support the complete connection of heterogeneous devices. Compatibility problems are widely discovered in the products and services of IoT enterprises, thus as an important hindrance to the future development of IoT.[1] In order to improve the interoperability of their products, IoT enterprises need to technologically adjust their products at multiple levels such as operation platform, communication protocol, data processing and application model, so as to solve the problems of protocol conversion, network connection and network management in the connection of heterogeneous devices.

Likewise, improving the expansibility of existing IoT devices and expanding the physical boundary of IoT is the main direction of the future development of IoT. The expansibility of the IoT system means the capacity to add new devices and services to the IoT system without reducing the performance of existing IoT services, which requires IoT enterprises to build a central-control system with massive storage space, efficient processing capacity and high compatibility to support the effective access, application and maintenance of external expansion devices of the main network system of IoT.

Besides, IoT enterprises need to take efforts to solve security risks resulting from the expansion of devices to the main network. For example, by establishing an encrypted security-trust mechanism and inspecting the security of the expansion devices, they can prevent the main network from suffering from network virus attacks and losses to IoT systems and enterprises because of data connection between external devices and the main network.

3. The Contradiction between Outdated Policies and the Application of New Technologies

In recent years, IoT security incidents have occurred frequently in various countries, which have urged governments to timely publish laws and regulations to supervise IoT security and strengthen IoT security protection. However, as the application of new technologies stimulates fast industrial transformation, various countries face multiple pressures to formulate regulatory policies, and regulatory policies per se lack latitude. Consequently, the development of the IoT industry falls into the predicament in reality, or Collingridge´s Dilemma. The structural contradiction between the existing regulatory policies of governments and the application of new technologies seems hard to be eliminated. It has a negative impact on the future development of IoT industries and enterprises.

(1) Traditional regulatory models restrict the development of emerging technological industries.

1. Jing Q, Vasilakos A V, Wan J, et al. "Security of the Internet of Things: perspectives and challenges." [J] Wireless Networks, 2014, 20 (8): 2481-2501.

The rise of IoT as an emerging technology signifies a "destructive process of creation" , and corresponding governmental regulatory measures and thoughts keep pace with the times. Suppose governments only adopt traditional regulatory models in emerging technological industries. In that case, they will ignore the problems of technological security, industrial development efficiency, personal privacy rights and social stability in the industry.[1] Therefore, as the main body of regulation, governmental agencies should change their regulatory thoughts, innovate regulatory measures, and respond to the development challenges of the IoT industry with the regulatory framework represented by adaptive regulation.

However, countries now lack governance experience of emerging technologies. The United States, the European Union and the United Kingdom still take inertial traditional legal regulations and the minimum industrial standards as the main measures to meet the challenges of IoT development, which proves unsatisfactory. For example, the *Internet of Things Cybersecurity Improvement Act* in the United States raises the requirements for vulnerability sharing within the federal government and between suppliers and the federal government, as well as preliminary provisions on periodic audits and measurement. Since the sharing of vulnerabilities first needs to realize the sharing of asset information, which will inevitably involve sharing manufacturers' information. The vulnerabilities collected by the US government through the Act may endanger the core business interests of enterprises and violate relevant laws of other countries. In the future, governments must consider how to establish an adaptive regulatory system, i.e. how to assist technological innovation, prevent and control industrial risks, and ensure that main enterprises serve the public interests.

(2) The existing policies lack latitude in dealing with the application of emerging technologies.

When formulating regulatory policies on IoT, various governments generally face the adaptability of regulatory policies. If governmental policies seem too flexible and lack regulatory effectiveness, security problems that arise from industrial development may do great damage to society and emerging industries. However, in case of the lack of latitude for industrial development, the development of enterprises and the iterative innovation of technologies will be impeded and the new business form of new technology cannot be established.

Presently, countries raise IoT security to the level of national security, generally adopt strict regulatory policies and punishment measures, and excessively pursue the absolute security of technology and data protection, so much so that in terms of cybersecurity regulations, various countries commonly encounter practical problems of low latitude for the application of emerging technologies, simple requirements for standard formulation and rigidity in implementation. For example, the provisions of *The Security of Connected Devices* (SB-327), which came into force in State of California (the US) in 2020, clearly stipulate that device makers shall bear the responsibilities for privacy security and device security, yet do not optimize specific provisions of the responsibilities,

1. Xue Lan and Zhao Jing. "Towards Agile Governance: Research on the Development and Regulatory Model of Emerging Industries." [J] Chinese Public Administration, 2019 (08): 28-34.

privacy security and device security, yet do not optimize specific provisions of the responsibilities, just using "security procedures" appropriate to "reasonable measures" to interpret the security responsibility of device makers.[1]

(3) The compliance requirement allows for no flexibility and does not take into account the actual operation of enterprises.

The Security of Connected Devices (SB-327) only emphasizes the regulation and does not take into account the actual operation of enterprises. For example, its provisions allow for no flexibility in compliance requirements and make the same compliance requirement for different device manufacturers. As a result, corresponding compliance provisions cannot meet the security standards of complex devices, and increase the compliance costs of simple devices, causing great controversy among IoT enterprises. In addition, the *2020 Guidelines for Securing the Internet of Things* released by the European Union Agency for Cybersecurity (ENISA), *The Code of Practice: Securing the Internet of Things for Consumers* issued by the Australian government and *Comprehensive Countermeasures for Internet of Things Security* published by the Ministry of Internal Affairs and Communications of Japan in 2017 all have the problems of vague policy-content, rigid-uniformity compliance provisions and inflexible review mechanisms, which nag and challenge IoT enterprises that hope to improve their compliance standards.

Simultaneously, the punishment measures of regulatory policies in various countries tighten the grip. For example, the *General Data Protection Regulation (GDPR)* of the European Union stipulates that enterprises that violate data protection provisions will face a top fine of 4% of their global revenue or 20 million euros. The final and provisional fines for violations stipulated in *Securing the Information and Communications Technology and Services Supply Chain,* a presidential executive order of the United States, include civil penalties and criminal penalties: civil penalties can be imposed with a maximum fine of 250,000 US dollars (subject to inflation) and criminal penalties can be imposed up to a fine of one million US dollars and up to 20-year imprisonment or both.

(4) The normal state in which policies lag behind technological development.

Governmental policy regulation in the field of IoT security has also fallen into the control of Collingridge´s Dilemma. IoT constitutes a part of the entire economic and social structure, and the control of regulatory policies over technological development weakens. Collingridge´s Dilemma is proposed by British technology philosopher David Collingridge,[1] which observes that it is challenging to predict the future of technology in the early stage of technological development, though people have relatively high control over it then. However, when people have understood the consequences of technology, their control over technology will become extremely limited, because technology has obtained enough power and formed its own development path.[2]

In the early stage of the development of IoT technology, IoT technology just stays in the test

1. Collingridge D. The social control of technology [J]. 1982.
2. Jane Calvert. "Governing in the Context of Uncertainty, " Synthetic Future: Can We Create What We Want Out of Synthetic Biology?. special report, Hastings Center Report 44, no. 6. 2014: S31-S33.

of R&D personnel, when the development of IoT technology embodies great correct ability, controllability and selectivity. R&D personnel can timely adjust technological vulnerabilities at the technological level, hedge against negative effects, and control the development direction of IoT.

However, after IoT technology fully develops, or is widely used or deployed in various sectors (as an important part of the entire social operation mechanism), IoT development forms its own evolution path and the effectiveness of policy regulation gradually weakens. Meanwhile, as IoT has been deeply embedded in social infrastructure, any technological adjustment and hardware deployment will have a significant impact on the entire society. Force policy-makers to consider the social impact of regulatory policies, which certainly incur the control dilemma of policy regulation on IoT technology, increase the difficulty of governments in formulating regulatory policies and obstruct corporate technological innovation.

4. Geopolitical Games Complicating the Landscape of IoT Security

European countries and the United States carry out the scrutiny of security on supply chains based on the Pan-ideology of national security on the grounds of national security, which blurs relevant legal boundaries and poses greater compliance challenges to the operation of transnational IoT enterprises.

(1) Pan-ideology of national security means a more complex compliance environment for IoT enterprises.

Governmental cybersecurity policies take into account national interests, emphasize national security, and implement relevant security measures. Therefore, the political stance of the Pan-ideology of national security leads to obvious differences and blurriness in political review, regulatory emphasis and review discretion of security policies issued by some countries, resulting in a more complex policy-compliance environment. IoT enterprises have to face multiple-level security reviews.

First, foreign IoT enterprises are regarded as competitors and prevention targets. In recent years, IoT security has constituted a major source of threat to national security. Most countries highlight national security in policy making and regulatory direction. When they draw up security policies and regulatory measures, they see foreign IoT enterprises as competitors and prevention targets, or even coerce foreign enterprises into a geopolitical game. The coercion of the political game will affect the formulation of international IoT regulatory systems for a long time. Policy direction that overstates national security and risk aversion will inevitably have a negative impact on the effectiveness of policies.

Second, the laws and regulations promulgated by various countries feature overt national differences. Countries' security policies have obvious differences and blurriness in political review, regulatory emphasis, and review discretion, resulting in a more complex policy-compliance environment. IoT enterprises have to face multiple-level security reviews. Countries accelerate the review of communication technology and service transaction in key fields like wired devices and UAV systems, which will directly affect the normal operation of relevant enterprises in the world.

Besides, countries issue relevant regulations and executive orders to strengthen the identification and evaluation of information, communication technology, and service transactions involving foreign application software and establish a new set of review-regulation processes to review foreign applications as required. Under such a circumstance, relevant foreign science and technology firms have to face more data reviews based on ideological discrimination.

(2) Security review based on political factors restricts the internationalization of IoT enterprises.

In political review, the compliance standards of IoT security policies of various countries comprise not only technological security standards, but also geopolitical factors that various countries take into account. As a result, IoT enterprises have to face the review of technological security standards and the political review of market countries as well, which means that though IoT enterprises can meet compliance standards in terms of technological security, they probably face political reviews and all-round governmental sanctions therefrom or even withdraw from the market.

First, in terms of the review, countries aim to ensure their national security and economic security in formulating IoT security policies. For example, countries explicitly ban the transaction and use of foreign information and communications technology or service (ICTS) that may pose a special threat to their national security, diplomacy and economy. This compels IoT enterprises to avoid potential risks of their products and services to national security and economic security in the face of national security review. A series of legislative work on IoT security arouses worldwide attention. The European Union, Japan and Australia have also accelerated their legislative process on IoT security and gradually established their regulatory systems. For example, generally speaking, the EU′s cybersecurity policy embraces the protection of data security and infrastructure security, and highlights the protection of personal privacy data and infrastructure stability by IoT enterprises. The differences in regulatory priorities between Europe and the United States have multiple-level impacts on the market operation of IoT enterprises. For example, when IoT enterprises march toward European and American markets, they need to design and apply products in line with different compliance standards to meet different regulatory priorities of the European Union and the United States. This undoubtedly increases the cost or investment of enterprises in corporate compliance, puts more pressure on the operation of enterprises, and poses challenges to the long-term development of enterprises.

Second, in terms of review discretion, the compliance content and discretion right of IoT security policies in various countries remain vague now, increasing enterprises' violation and legal risks. As countries stay in the early stage of exploring and formulating IoT security policies, most of the cybersecurity policies belong to guiding documents without clear regulatory and legal boundaries. In the meantime, the implementation regulators of various countries develop in the early review stage, and own great discretion right in the implementation of standards and specifications. As the review results mainly rest with the independent discretion of law enforcement agencies, IoT enterprises remain the role of underdog in the face of compliance review by relevant agencies, and may fall into compliance risks at any time, which have a negative impact on the operation of enterprises.

Third, in terms of review scope, the review of foreign IoT devices is reinforced from the process of procurement. While strengthening the security provisions of domestic IoT devices, national laws also start stricter reviews of the procurement of foreign IoT devices. The procurement clause in the Internet of Things Cybersecurity Improvement Act of the United States stipulates that if the use of IoT devices will prevent federal government agencies from complying with device-security requirements and vulnerability-disclosure guidelines, relevant devices are prohibited from being purchased by agencies, unless there are exemptions such as scientific research purposes.[1]The Comptroller General of the United States performs his duty to submit the implementation report of procurement terms to United States Congress every two years. Generally speaking, due to the differences and blurriness of national cybersecurity policies, IoT enterprises must not only formulate self-examination mechanisms according to security-policy standards of different countries and increase their investment in technological compliance, but also adopt appropriate business models and political lobbying to deal with the political review of enterprises by various countries, dispel political suspicion and avoid sanctions and delisting. This certainly means more compliance costs and challenges to enterprises.

(3) The absence of international cooperation causes unknown risks to the global operation of IoT enterprises.

International cooperation serves as a necessary way to reduce geopolitical risks related to IoT. In recent years, the international community has achieved remarkable progress in collectively combating cybercrimes, which has yielded unsatisfactory results yet. The problems are mainly as follows.

First, the lack of an international coordination mechanism for cybersecurity policies in various countries cannot achieve cooperation in global governance. Indeed, governments of various countries have accelerated the legislative process of cybersecurity and improved the construction of relevant laws and regulations. Owning to different national conditions and legislative demands of various countries, the awareness of common governance in the formulation of cybersecurity policies remains absent, so much so that the existing policies of various countries lack an international coordination mechanism, which fail to forge global governance and reduce the effectiveness of policy governance in various countries. Taking cross-border data protocols between Europe and the United States as an example, in July 2020, the European Court of Justice affirmed that the United States did not provide EU data subjects with the data rights that can be actually exercised and the corresponding judicial remedies, which violated *Charter of Fundamental Rights of the European Union,* thus ruling that *Privacy Shield Agreement* was invalid. This directly bogged down data transmission of cross-border enterprises in Europe and the United States, restricted the global operation of enterprises, and caused economic losses to bilateral enterprises.

Second, the lack of universal standards for global IoT cybersecurity leads to the absence of

1. Zhang Xiye. "Trends of IoT-Security Legislation in the United States and the Inspiration to China." [J] China Internet, 2021 (06): 32-37.

consensus. Regarding combating IoT cyber threats, the international community has signed regional and bilateral treaties. For instance, *Budapest Convention on Cybercrime* adopted relevant provisions on cloud access to electronic evidence in 2017, so as to quickly identify the perpetrators of IoT attacks. Shanghai Cooperation Organization also stipulates relevant provisions on combating cybercrimes. Yet, universal standards at the United Nations level have not taken shape. *Convention on Combating Cybercrimes* under negotiation faces many obstacles too, which demonstrates the serious lack of consensus among countries on cybersecurity and universal security and hinders international cooperation in the field of IoT security. This directly gives rise to the fact that IoT enterprises commonly encounter numerous cybersecurity risks when they partake in global operations.

Relevant cases occur occasionally. For example, in March 2021, the camera supplier of Tesla factory was hacked, with a total of 150,000 monitoring access rights of many institutions being obtained. In May 2021, security vulnerabilities were revealed in Qualcomm's Mobile Station Modem (MSM) chips, which affected 40% of global mobile phones. Colonial Pipeline, the largest fuel transportation pipeline corporation in the United States and JBS Group, the largest meat supplier globally, was blackmailed, with short-term tight supply of oil and meat and great impacts on the global economy.1Presently, the development of global IoT security evolves with a new trend that features frequent security incidents of ransomware attacks, the extensive scale of data leakage and continuous emergence of major security vulnerability, which forms potential risks and negative impacts on the long-term development of IoT enterprises.

Third, a motley collection of standards curbs the interconnection of IoT. The rapid development of IoT stimulates the demand of manufacturers and other enterprises for global deployment. Enterprises hope to realize rapid global access and unified deployment management of their terminal devices.[2] In the meantime, countries and regions generally incorporate their own priorities into the formulation of IoT standards, which provokes substantial divergences in IoT standards among countries and forces device manufacturers to comply with numerous governmental and industrial standards while meeting market demands. This raises the threshold of corporate compliance and digresses from the endogenous requirement of IoT “interconnection”.

Fourth, the lack of trust counts against concerted action in face of cyberattacks. Currently, cyberattacks on IoT are characterized by a wide range and enormous impact. An enterprise or a country can hardly cope with global threats by tapping its own resources. Various countries need to take more measures at home and abroad to coordinate relevant work. Now private sectors set up many good models for cooperation, including developing technology and risk management standards, organizing information sharing forums and so on. However, coping with super-large-scale cyberattacks requires national cooperation. In particular, various countries adopt different stan-

1. Hufu Think Tank. Global Cybersecurity Policy and Trend Report in the First Half of 2021. [EB/OL]. [2021-08-24]. https://www.secrss.com/articles/33748.
2. paper.cnii.com. “IoT ‘Global Connection’ Collaboration Initiative Has Received Positive Response from Global Operators.” [EB/OL]. [2017-06-28]. http://www.chinaunicom.com/issue/detail-gsma12.html.

dards, regulations and terminologies. The reality necessitates improving cooperation in threat intelligence, incident reports, best practices of risk resistance and response measure and crisis exercise, to strengthen cooperation on cybersecurity. However, as some countries pursue hegemonic acts and alliance acts in cyberspace, the lack of trust among major powers counts against concerted action in face of cyberattacks, which embodies the most important impact of the geopolitical game on cyberspace now.

Chapter 4

The Best Practices of IoT Security

1. IoT Security Certifications

IoT devices create lots of data, such as logs and metrics, that can be monitored and analyzed to not only monitor performance but also preemptively discover and troubleshoot vulnerabilities and other security issues.

IoT has become potential target of cyber-attacks more and more. Preventing the next big attack means implementing best practices and using the right tool set. Logz.io Security Analytics, for example, enables users to identify potential threats based on what is happening both inside the system and in the world outside the corporate network. Capabilities such as threat detection and correlation rules enable users to monitor IoT devices and identify attack patterns as they are taking place.

（1）IoT security certifications

Certifications by specific organizations help device makers and users prioritize building-in product security and focus on consumer trust and confidence.

For IoT products and IoT solution providers, there are kinds of information security and privacy certification/validation with the consultation of various global agencies, and now serves as an with international certificates, including:

ISO/IEC 27001 Information Security Management System Certification (ISMS), ISO/IEC 27017 Certification for information security of cloud services

ISO/IEC 27701 Certification of privacy extension to ISO/IEC 27001 Information Security Management and ISO/IEC 27002 Security Controls.

CSA STAR Certification for cloud security

EU GDPR Validation Program

US California Consumer Privacy Act (CCPA)

ETSI EN 303645, a European Standard on cyber security initiatives in consumer IoT security.

Platform Security Architecture, first introduced at Embedded World in 2019. At the time, seven of the leading security companies (Arm, CAICT, Riscure, Prove and Run, SGS Brightsight, TrustCB and UL) came together to introduce a certification that was the first of its kind: certifica-

tion based and unpinned by the PSA Certified-RoT.

IEC 62443

IEC 62443 is a series of internationally recognized standards that specify the process and product requirements for the secure development of Industrial Automation and Control Systems (IACS). It therefore addresses Industry 4.0 operators, system integrators and product manufacturers and their compliance to cybersecurity best practices.

In particular, the IEC 62443-4-1 (process related) and IEC 62443-4-2 (product related) standards highlight the importance of choosing vendors that provide hardened hardware components built with a "security by design" approach, ensuring that security best practices are followed throughout the entire product lifecycle, from PoC to full production to decommissioning phases.

(2) IoT security considerations

IoT is incumbent upon device manufacturers, as well as the enterprises using these devices, to understand their roles in keeping devices and users secure. If both manufacturers and users begin to implement better practices in these technologies' nascent stages, a great deal of future damage can be avoided. While achieving total security for all IoT devices probably isn´t realistic, the overall scope of damage can be avoided by implementing the right tools and best practices.

Standardization and certification: aligning a unified approach to security throughout. The data that is being gathered by IoT devices enables business leaders to make more informed and timely choices, but they need to know that every device that is generating information has a consistent level of security built-in.

If devices come from different manufacturers, that all work to their own security standards, there will be no consistency in the approach or implementation, and leaders will struggle to understand and trust the devices. Also, inconsistency puts IoT networks at risk, leaving them vulnerable to attack.

Device makers should ensure a consistent standard of security is designed-in to the hardware and firmware of all devices. The ecosystem has an important role to play in this. We all need to work together to identify and share industry best practice, so we can overcome current and future security threats and make sure everything is built on a common foundation of security.

Right-sizing security to minimize downtime. As the costs of security are determined by the number of measures needed to adequately protect a device, and the number of assets in need of protection, manufacturers must be able to identify the right level of security for their product. This will help OEMs avoid under- or over-investing in security. Designing-in security from the outset will also save time and costs associated with patching or retrospectively fixing hardware security issues.

In addition, using certified components will help device makers reduce the total cost of ownership because security has already been built in. The benefits extend to customers as well - trusted frameworks, and drawing on industry best practice, will help OEMs minimize downtime in their operations.

Security-by-design for IoT devices. To build security into a device, providers should consider

how they will, for example, avoid cloning and reverse engineering, and protect their product from software and hardware attacks. That means security should be implemented in the early stages of the product development lifecycle.

Supply chain security. As we connect more devices, the attacks surface will continue to grow, and attempts to access products and data will become increasingly sophisticated. However, more often than not, hackers will take the path of least resistance. That is why security patches are so important. Hardware security is difficult to update, so device makers should ensure security is built into a device from the ground up. Security should also be implemented and work seamlessly across all layers.

It is also vital that security is available and affordable throughout the device lifecycle While product lifecycle management and patching are complex and expensive, retrofitting is very costly, time-consuming, and complicated.

Prioritizing security to build consumer trust. The IoT has captured consumers' attention. The number of devices in the average household also increased, along with homeowners' intention to buy at least one product.

2. Case Studies

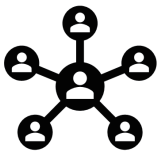
2.1 How certification can help improve cybersecurity for Industrial IoT Applications

The data gathered by the Internet of Things (IoT) devices could make even the most well-established industries more efficient, productive, and sustainable. However, the same connected technologies could also put asset owners and operators at risk. As industrial IoT (IIoT) applications (such as manufacturing, agriculture, construction, energy, utilities, medical and transportation are being transformed), cyberattacks are becoming increasingly more common–not only in cases where devices are decades old, with hardly any security measures built-in.

Eurotech is a multinational company that designs, develops and supplies Edge Computers and Internet of Things (IoT) solutions - complete with services, software and hardware - to system integrators and enterprises. By adopting Eurotech solutions, customers have access to Iot building blocks and software platforms, to Edge Gateway to enable asset monitoring and to High Perfomance Edge Computers (HPEC) conceived also for Artificial Intelligence (AI) applications.

Integrated hardware and software

Network Security Design



End-to-end network security

Figure Eurotech's cybersecurity by design approach

Eurotech´s ReliaGATE 10-14 and Everyware Software Framework have been PSA Certified, ensuring standards-based security compliance for IoT deployments

This certification highlights Eurotech´s commitment towards providing IoT building blocks

compliant with the latest cybersecurity requirements and regulations. We are very proud of having achieved the PSA Certified Level 1 and being able to offer trusted IoT solutions with a designed-in security approach.

PSA Certified Level 1 is an important milestone of the Eurotech IoT security roadmap and another step that helped us achieve IEC 62443-4-1 and IEC 62443-4-2 certifications.

2.2 Case Study of Seoul-based SDT Inc: Cybersecurity for Smart City Applications

In smart cities, Internet of Things (IoT) devices are being used to check for hazardous conditions or signs of wear and tear. For example, city administrators can use smart sensors to monitor the temperature, humidity, water level, gas concentration, and oxygen saturation levels under manholes. The data these devices gather helps to protect workers from potentially dangerous situations and provide predictive maintenance information on utility networks.

With safety-critical environments, the infrastructure operator must be able to trust the data that is being gathered, which means it must come from a trustworthy device. Seoul-based SDT Inc. offers a secure foundation on which IoT developers can build new smart city applications. SDT´s smart city solution includes system-on-modules for SDT smart hubs, and integrates with operating systems, connectivity, security, and cloud services to provide the starting point for a range of applications.

Security risks considering smart cities

As more and more connected devices are deployed, countless new business opportunities will be unlocked. However, the current insecurity of IoT devices means that risks will also rise. With increasing demand from consumers, governments and the wider IoT industry for a universal baseline of requirements, independent IoT security certification has never been more important.

Security of Smart City and the IoT

The IoT is crucial to achieving a smart city´s aims because it provides the fuel a smart city runs on, that is, the data. That information is then used to deliver fresh insights into all aspects of city life, from the ground up and drive improvements. For example, a program to install smart traffic signals in the US city of Pittsburgh has been expanded after initial research found adding sensors to existing equipment reduced the wait times at intersections by more than 40%. Similarly, building automation can transform workplaces, improving entrance management and minimizing energy consumption.

To help build trust and assurance in the devices that will underpin the smart cities of the future, industry experts have developed PSA Certified: a global partnership providing a comprehensive framework and independent certification for IoT security implementations. Ecosystem of PSA Certified silicon and system software is simplifying security for device manufacturers, allowing them to leverage the expertise of the value chain. PSA Certified also provides mapping to major IoT security standards and regulations, including ETSI EN 303 645, NIST 8259A, and Californian State Law SB-327. Similarly, customer can reuse PSA Certified Level 1 certification in other schemes, enabling alignment with end-market requirements and guidelines.

SDT has five PSA Certified products using STMicroelectronics silicon, which are all based on

Arm architecture. This means SDT has followed a four-step security framework to ensure its products are developed in line with industry best practices. PSA Certified also assures that world-leading laboratories have assessed the device as having the right level of security of built-in.

2.3 Tuya Smart (NYSE: TUYA), A Practical Case of IoT Security

After a full day of meetings on a business trip, you arrive at your hotel, tired and looking for a quick refresh and good nights rest. You are greeted first by a smart robot in the hotel lobby for a facial-recognition hotel check-in, avoiding the long line at the reception desk. Upon entering the elevator, it automatically identifies your floor. Within three minutes, and without fumbling with your hotel key you arrive at your room. You enter your room, equipped with over 20 intelligent devices powered by Tuya that combine together for various scenes and voice-applet wake-up and controls. Users are able to turn on room lights and close the curtains, all from the comfort of bed. In the hotel, various smart devices interconnect and organically integrate in private and public spaces.

After your business trip, you arrive at your apartment entrance, where lights automatically turn on as the system identifies you and unlocks. You no longer have to search for your keys in your bag at night. Since the residential community installed an intelligent lighting system inside and out, you have saved 20% of your monthly electricity bill. With the intelligent trash-thrown-from-high-window monitoring system installed in the community, you don´t have to worry about whether children are hit by sudden objects when playing on the outdoor ground.

As you open the door to your apartment, warm yellow lights and your air purifier turn on automatically, while your water heater is activated to a comfortable temperature in advance according to personalized settings. Having taken a bath, you feel comfortable. Just say “good night,” and your lights switch off, curtains close, and doors and windows are locked for the evening. When you wake up in the morning, simply say “good morning,” and your curtains open and morning music plays automatically, starting the day with positive energy.

Many years ago, the above-mentioned scenes could only be imagined in movies. However, with the development and popularization of IoT, 5G, cloud computing, and other technologies, interconnected intelligent scenes are no longer difficult to achieve.

Be it smart communities, smart hotels or smart homes, all are linked with the security and well-being of thousands of households. Therefore, Tuya Smart designs multiple security-guarantee measures across its ecosystem to ensure the security and reliability of IoT devices in various scenes.

Hardware Product Security and Quality-Guarantee Solution

Intelligent hardware has long supply chains and diverse product types. Taking cost into account, product expenses can vary substantially, resulting in a large gap in the computing capacity of product chips. Traditional information-security standards are not fully applicable to intelligent hardware, which requires IoT manufacturers to organize strong professional information-security teams and participate in the design, execution, production, and upgrading of the entire IoT products. This significantly increases the security cost of intelligent hardware.

For example, in 2022, Tuya Smart launched WBR3N, a built-in IoT security module, which takes a security chip certified by "CC EAL6+" as a root of trust, with industry-leading security-capacity support. The module possesses a comprehensive security guarantee. In addition to the built-in ECC security certificate and device authentication information into SE in production, WBR3N actualizes two-way certificate authentication and device-activation authentication between device and cloud-end. In terms of communication, WBR3N adopts TLS two-way strong verification communication based on security authentication, which boasts the highest level of communication-security guarantee in the industry now.

In the protection of device-data security, WBR3N performs the process of data encryption and decryption via the built-in independent SE to fully ensure data security. Simultaneously, WBR3N provides independent physical security storage based on SE and has a built-in root of trust to encrypt the storage via it. Similarly, the built-in SE protects the core code, and OTA ensures process security based on secure communication process and firmware verification.

WBR3N is equipped with multiple logical and physical protection layers like metal shielding, end-to-end encryption, memory encryption and tamper detection, which can effectively defend against various advanced attack means like power analysis and fault attack.

Tuya Smart is one of the earliest IoT platform service providers pursuing IoT information security solutions. Since its establishment, Tuya Smart has set information security as the core bottom line of its intelligent product solutions.

Enhancing the Control of R&D-Security Process to Ensure Product Security and Quality

In order to control the security and quality of intelligent hardware products, Tuya Smart has established a professional information-security team of more than 20 people in-house to control the software development life cycle (SDLC). It strictly applies a secure SDLC to develop services and products at three ends, i.e. cloud, app and intelligent device, which incorporates information security into the lifecycle of software development. The lifecycle of software development of Tuya Smart comprehensively covers all stages of the system development lifecycle, aiming to guarantee

the security of every line of code by controlling various processes and means.

Tuya Intelligent Security Team fulfills unified project-SDLC-implementation monitoring and management via a security-management platform, and realizes fully-automated process tracking and the whole-process security review, testing and delivery.

In order to ensure the foresight of technological practice in the security R&D of intelligent products, Tuya formulates security-classification standards of intelligent hardware devices that are internally developed based on global industrial information-security standards (including but not limited to ETSI EN 303645, NIST IR 8259A, ioXt Alliance Security Checklist, etc.) and implements mandatory security requirements based on different types of products.

In line with the security-baseline requirement and security-technology planning, the Team compiles corresponding security-test cases to ensure the enforceability of security-technology from planning to verification as well as the effective implementation of security planning.

Actively and Intelligently Identifying Security Threats and Taking Preventive Measures

Tuya Sage, an IoT security-operation platform of Tuya Smart, aims to help developers identify and eliminate potential security risks of the IoT system and ensure security compliance in the operation of the IoT system.

Sharing joint security responsibility is the core principle of IoT security. IoT platform service providers undertake the responsibility of security management and operation of services and data interaction on the cloud platform and of the security of cloud-service platform and basic architecture. When developers independently develop their apps or hardware-embedded software (including using SDK) and business systems to access cloud platforms via API, they need to ensure the security compliance of their apps and data, including hardware and apps. However, in practice, many developers lack the entire perception of the security and compliance state of global intelligent terminals, which forms a common problem in the IoT industry.

On Tuya Sage, developers can see all protected devices, including the state of basic security information and risks. Once devices are attacked, developers can complete risk-interception with one click. With real-time threat intelligence, Tuya Sage can timely and effectively identify local vulnerabilities of intelligent terminals, enabling developers to fully understand the compliance state of terminal security and privacy and discover the non-compliance flow of user data to deal with it at the first time.

Strictly Implementing the Principles of Secure Data Processing and Storage Worldwide

For Tuya, protecting user data has always been one of its core missions.

Globally, Tuya owns six data centers, based in Oregon (the U.S.), Virginia (the U.S.), Frankfurt (Germany), Amsterdam (the Netherlands), Mumbai (India) and Shanghai (China). Simultaneously, in order to provide better services to customers in more countries and regions in the world, Tuya will continue to build more data centers in the future. Each data center deploys independently in the market segment.

As a service provider and data processor, Tuya is the consignor of client-data processing. It signs strict data-processing agreements with clients, including responsibilities and obligations like

data-processing scope and data-processing models. Tuya has strict internal access-control strategy and technological-guarantee architecture. Only with the authorization of clients can it access or process data.

In all Internet-based interactions, Tuya uses TLS for secure communication, and conducts additional AES128 encryption for data content. In data storage, Tuya uses AES256 encryption or SHA256 Hash to de-identify data before storing in cases of all users sensitive data.

Tuya carries out data collection in line with basic principles of protecting data and personal privacy rights. User consent to data collection is the most important legal basis. Tuya collects data by ensuring the user right to know and necessary service principles. In data collection, the R&D process follows a PIA/DPIA procedure to analyze the protection lifecycle of personal data and ensure the legitimacy and compliance of data collection.

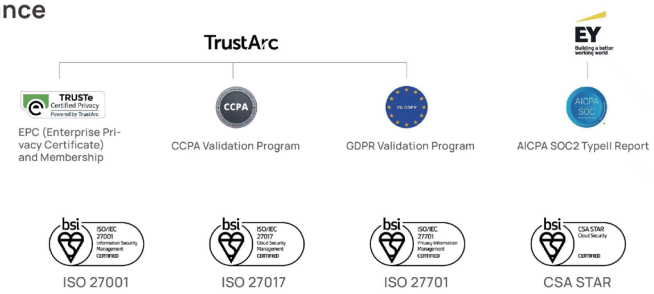
Cooperating with Top International Third-Party Institutions in Security&Compliance Assessment/Certification/Validation/Testing/Audit

In recent years, Tuya Smart has done its utmost in security and compliance for platforms and technologies and actively carried out third-party data-security assessment/certification/validation/-testing/audit to meet the needs of global clients. This is in tune with the development orientation of Tuya Smart, a global IoT development platform service provider.

So far, Tuya Smart has obtained some mainstream information security standards and compliance requirements in the market. Simultaneously, Tuya has been endorsed by a well-known international organization: ISO series of certification and CSA STAR of BSI. Now, Tuya has passed the validation report of GDPR, optimized the security protection and compliance requirement of personal data, and officially fulfilled CCPA privacy-compliance validation program and privacy laws in Canada, the PIPEDA/Québec Bill64, by cooperating with TrustArc, an international well-known privacy and compliance consulting institution. An annual external audit conducted by E&Y explains Tuya's continuous effort in seeking an independent eye of Tuya internal security and compliance implementations. Besides, on the basis of intelligent hardware solutions, Tuya has obtained EN 303645 and NIST IR 8259A certification of TÜV SÜD, as well as the security certification of ioXt Alliance. All of these demonstrate that the existing product solutions of Tuya fully comply with industrial information security standards.

Additionally, Tuya has invited information security corporations including Rapid7, Underdefense, ScienceSoft, Wizlynx Group, Chaitin Tech and DAS-Security to test the information security capacity of its products with their professional penetration tests.

- Compliance



- Security

Chapter 5

The Initiatives to Safeguard Global IoT Security

IoT security plays an important role in maintaining global cybersecurity. In IoT security, various countries encounter not only technological challenges but also the risks of national-policy coordination and supply-chain decoupling. "Multilateral Cyber Action Committee" of Center for Strategic and International Studies (CSIS) of the United States released a report, stating that the competition among major countries coerced governments and private sectors into a more complex, ineffective and risky digital world.[1]The policy-making circle and academia have carried out in-depth exchanges regarding IoT security and achieved remarkable research results. For example, the sixth working group of *Paris Call for Trust and Security in Cyberspace published Secure ICT Supply Chain.* The report proposed establishing a policy framework in five aspects (i.e. public policy, technological standard, corporate governance, public-private cooperation and international cooperation) to strengthen the security of the ICT supply chain.

Meanwhile, influential scholars express profound opinions on the status quo of global cybersecurity. Paul Triolo confirms that the cold war on science and technology yields a lose-lose result for both sides, and that various countries need to forge a consensus on technology and national security, so as to slacken the control of technological flow. Therefore, a new international mechanism can be established to harness competition.[2]

In academic exchanges, Samm Sacks also stresses that "an evidence-based framework is desirable to assess national security risks to cope with the decoupling of science and technology between China and the United States."[3]

Graham Webster emphasizes that "Sino-US science and technology competition does not mean a science and technology cold war" and that "(Chinese) app bans won´t make US security

1. CSIS: The Two Technospheres[EB/OL]. [2022-3-29]. https://www.csis.org/analysis/two-technospheres.
2. Cliff Kupchan and Paul Triolo. Distrust but verify: How the U.S. and China can work together on advanced technology – SupChina[EB/OL]. [2019-11-26]. https://supchina.com/2019/11/26/distrust-but-verify-the-us-china-advanced-technology/.
3. See Samm Sacks' speech at "Digital Trust Virtual Roundtable" hosted by Research Center of Global Cyberspace Governance (RCGCG) on September 14, 2021.

risks disappear".[1]

Melissa Hathaway, a well-known expert in the field of global cybersecurity, keenly unmasks that the issue of cybersecurity is closely associated with the lack of capacity. Many organizations have not integrated cybersecurity into the development of digital infrastructure, or established necessary risk-elimination procedures to ensure the management of cybersecurity and technological risks.[2]

Experts interested in Sino-US cybersecurity take assiduous efforts to strengthen bilateral cooperation and maintain the stability of cyber relations.

Charles Barry reckons that China and the United States can fortify cooperation in the field of globally-shared key infrastructure, such as backbone network in the field of communication, maritime tracking systems in the field of transportation and SWIFT in the field of finance.

John C. Mallery observes that establishing a supply chain system with higher security standards can help maintain the stability of Sino-US cyber relations.

Considering the existing research results in the field of global IoT and cybersecurity, as well as the latest research findings of the *The 2022 Global IoT Security White Paper,* the Research Group calls on governments, industrial organizations, and enterprises to take measures and make efforts from the following 12 aspects to jointly safeguard global IoT security:

1. Build an International Environment of Mutual Trust

Countries and transnational IoT enterprises across the world should embrace cooperation and mutual trust for cybersecurity, work to remove the obstacles to mutual trust and step up international cooperation by building strategic partnerships.

2. Strengthen Guidance in Legal Compliance

Regulatory authorities should continue to improve existing legal frameworks, actively conduct forward-looking legislative research, guide the healthy and orderly development of the IoT industry with legal constraints, and strengthen regulation and governance. IoT enterprises should operate using best practice according to laws and regulations, respect personal privacy, protect data security, and effectively integrate innovation-driven development with risk containment.

3. Improve the Construction of Standard Systems

More efforts should be made to facilitate the establishment of industrial security-design principles with standard systems, adopt general security baselines, reduce security vulnerabilities, consolidate security protection in the lifecycle of IoT products and services, and comprehensively enhance the overall security capacity and service quality of the IoT industry.

4. Optimize the Construction of IoT Ecological System

Relevant parties should give full play to the role of third-party testing and certification institutions, prioritize suppliers with cybersecurity-protection capacity in cooperation, and form a

1. Graham Webster. App bans won't make US security risks disappear[EB/OL]. [2020-09-21]. https://www.technologyreview.com/2020/09/21/1008620/wechat-tiktok-ban-china-us-security-policy-opinion/.
2. Melissa Hathaway. Integrating Cyber Capacity into the Digital Development Agenda[EB/OL]. [2021-11-30].https://thegfce.org/wp-content/uploads/2021/11/Integrating-Cybersecurity-into-Digital-Development_compressed.pdf.

zero-trust security model for the IoT supply chain, so as to continuously elevate security-protection technology and capacity, provide users with IoT products and services with security commitment, and build a safe IoT industrial ecosystem.

5. Establish Risk-Response Mechanism

Under the guidance of regulatory authorities, stakeholders should take initiative to disclose risk vulnerabilities in a timely manner, formulate emergency plans and provide repair plans to minimize the impact of security risks and hazards. They should ally with other parties to actualize risk control and the maximum security benefits of the whole IoT industry and continuously build up user confidence in IoT applications.

6. Improve Corporate-Compliance Capacity

Enterprises should highlight cybersecurity, assemble security teams, improve information-security systems, strengthen corporate-compliance capacity and eliminate the security risks of the IoT system by perfecting management models, processes, tools and platforms.

7. Enhance Consumer Awareness for Safe Use

Interested parties should increase awareness of cybersecurity via various channels such as publicity, education and training, so that users can fully understand potential cybersecurity risks when applying IoT devices, and cooperate with IoT enterprises in effectively protecting personal privacy and data security.

8. Rigorously Implement Technological Solutions

It is advised that technological means be used to cope with IoT security threats for accelerated updating of IoT technologies and exploration of IoT security technologies, and that more work be done in R&D and application of IoT security technologies to boost the rapid development of IoT security protection techniques.

9. Build an IoT Security Industrial Chain

All players in the IoT industrial chain should build demonstration projects of IoT security application and construct an open, cooperative and win-win IoT security ecosystem.

10. Build Service Systems

Further endeavours are required to establish IoT security service systems, build IoT security business teams in IoT system operation and maintenance, emergency, disaster prevention and evaluation, and strengthen the capacity-building of IoT security services in security assessment, risk verification, emergency drill and security reinforcement.

11. Construct Lifecycle Security-Guarantee Systems

Security protection should be implemented in the lifecycle of IoT security management to help construct security-protection technology systems that cover all links in the construction of the IoT system. Security-management requirements should be specified in all links of IoT-system planning, analysis, design, development, construction, acceptance, operation and maintenance and abandonment.

12. Solidify the IoT Security Talent Pool

The advancement of IoT security requires a large and high-quality talent pool. Additional efforts should be put into cultivating professionals in IoT security and doing in-depth research on IoT security. On the other hand, relevant parties also need to promote and implement existing IoT security rules and standards to IoT practitioners, and internalize security standards as an essential part of IoT design and implementation.

Implementation of the twelve initiatives contained at the end of this comprehensive analysis would go a long way towards improving IoT security on a global basis. These improvements are urgently needed with the advent of autonomous vehicles and the fourth industrial revolution.Particular attention should be paid to the innovative ideas contained in initiatives 5 and 6, "Optimizing the Construction of the IoT Ecological System," and "Establishing Risk-Response Mechanisms." These recommendations extend the thought processes around cybersecurity in important ways not commonly found in many reports.

Bruce McConnell
-- Distinguished Fellow and Board Member, The Stimson Center

The “White Paper on 2022 Global IoT Security” provides an in-depth analysis of IoT security from the perspectives of law, technology and policy, and is a comprehensive way to further understand cybersecurity. The White Paper also focuses on technical factors, the influence of global geopolitics on IoT security, and proposes 12 innovative initiatives to strengthen global IoT security. The 12 initiatives should receive great attention acclaim for furthering the progress of global cybersecurity.

-- Tian Li, Professor and Director of the Internet Development Research Institution of Peking University

A comprehensive analysis of the IoT Security ecosystem worldwide that emphasizes the opportunities and risks of the emergence of IoT and its interactions with different aspects of our lives. I see of particular interest the detailed review of cybersecurity policies and standards for IoT, which shows the complexity of the global situation and the challenges that a corporation must face in order to ensure the compliance of products, platforms, and services with this fragmented ecosystem. That’ s why summaries like the one provided in this article and the support of cybersecurity compliance experts are key to guiding corporations and helping them identify synergies and optimize testing, certification, and compliance process as demanded by their internal QA programs and the applicable regulatory and industry requirements.

-- Rubén Lirio, Head of Product Cybersecurity Testing, DEKRA

RCGCG
网络空间国际治理研究中心
RESEARCH CENTER FOR GLOBAL CYBERSPACE GOVERNANCE

ioXt
internet of secure things

Contributed by

psacertified™