SAFETY&DEFENSE
Scientific and Technical Journal ISSN 2450-551X

Asian Cyber Security Standards

Mateusz J. KUCZABSKI

War Studies University, Warsaw, Poland;
m.kuczabski@akademia.mil.pl, ORCID: 0000-0001-9952-1188

DOI: https://doi.org/10.37105/sd.75

Abstract

The scientific considerations outlined in this article address the threat to the cyber security quality system arising from unclear security standards implemented by China. Over the past few years, the Chinese government has imposed almost 300 new national cyber security standards. These norms cover a variety of information and communication technology (ICT) services as well as products, including soft-ware, routers, switches and firewalls. This standardization increases the threat to the cybersecurity quality system, and the more the US places pressure on the west-ern world for Chinese companies investing outside China and on western firms trading in China, the more difficult the situation becomes. The aim of this assessment is to identify these threats, which are also difficulties encountered by West-ern companies trying to develop their operations in China in order to minimize them. The study was compiled as an analysis of Chinese cybersecurity standardization policy documents and their confrontation with the practice of foreign businesses and as an analysis of international reports and standardization documents on cybersecurity. The theoretical investigative methods used in this paper are: syn-thesis, analysis, abstraction and generalization.

Keywords: cybersecurity, safety standards, cyberspace, commercial defense, IT infrastructure.

1. Introduction

Seconded European Standardization Expert in China (SESEC) is a project co-funded by the European Commission (EC), the Secretariat of the European Free Trade Association (EFTA) and the three European Standardization Organizations (CEN, CENELEC and ETSI). Since 2006, three SESEC projects have been implemented in

China, SESEC I (2006-2009), SESEC II (2009-2012) and SESEC III (2014-2017). In April 2018, SESEC IV was officially launched in Beijing for 36 months. The SESEC project supports the strategic objectives of the European Union, EFTA and European Standardization Organizations (ESOs). The SESEC project aims to:

- Promoting European and international standards in China;
- Improve contacts with different levels of Chinese administration, industry and standards bodies;
- Improve the visibility and understanding of the European Standardization System (ESS) in China;
- Collecting intelligence, regulatory and standardization information (Xu, 2018).

Despite the many efforts to bring the requirements in the area of standardization closer between foreign countries and China, Chinese cyber security standards create a set of diverse challenges for companies outside China in the area of security. The Chinese government may use the standards to put pressure on companies to undergo "invasive" product reviews, where sensitive intellectual property (IP) and source code (even if there is no clear indication of disclosure) may be required for verification and testing. In order to meet certain standards, foreign companies may be required to redesign products for the Chinese market if they do not comply with their domestic (Chinese) standards. In March 2018, The Office of the U.S. Trade Representative (USTR) issued a report on the discrimination and intellectual property (IP) challenges faced by U.S. companies operating in China, for which the Chinese market is particularly difficult. The difficulties are aggravated by the tightened US trade policy towards China. Retaliation with the use of standards, or rather the ambiguity of regulations, encourages discrimination against American and other foreign (western) entities. Chinese domestic standards build a competitive advantage for Chinese operators for two reasons:

- First, Chinese companies do not need to fear, unlike foreign companies, the obligation to provide sensitive information to the government as a condition for meeting standards.
- Second, Chinese companies may consider Chinese companies more secure on the basis of unclear criteria in the standards only because they are local and perceived to be more "controllable" and not influenced by foreign governments (something that China suspects foreign technology, whether true or not).

Although officially most standards are considered "recommended" (optional standards), in practice, for many entities may mean that they are required to meet them as necessary for doing business in China. This is the case when standards are listed as requirements for public or government procurement. In addition to government customers, some Chinese customers are not allowed to buy from suppliers who are not certified in accordance with certain standards.[1]

The standards are also becoming mandatory (obligatory) in combination with additional provisions that relate to these standards.[2] The government can audit companies for standards, even if the standards are not officially required. This, from a sales perspective, can generate significant costs for companies.

[1] This can be troublesome, because often the requirements vary greatly from company to company or product to product. There were cases in which contracts with customers were not concluded because, for example, the product did not have a specific certificate, and such a certificate was required.

[2] This practice is also valid in other countries. If appointments are made, e.g. in official documents, the standardization requirements become obligatory.

The ICT Market in China report reports that in 2014, the Ministry of Industry and Information Technology (MIIT) and Shanghai's municipal government jointly released a policy that opens opportunities in telecommunications for foreign companies in China in the (Shanghai) Pilot Free Trade Zone. The government's explanation of this new policy stated that foreign companies shareholding of information service business (app stores and data storing and forwarding) is no longer limited. The shareholding of online data processing and e-commerce was increased up to 55%. Furthermore, businesses in call centers, multi-party communication, internet access services, and virtual private networks (VPNs) were opened to foreign companies without shareholding restrictions. Other ICT sector regulations depend on the industry itself; for instance, in the software and hardware sectors, regulations are based on content and usage. For example, on 1 May 2015, the Local Administration for Industry & Commerce (AIC) and the Municipal Commission of Transport launched an investigation of Uber's Guangzhou office (and later its Chengdu office), as the Guangzhou province considers car-hire services that use private drivers illegal. They are therefore investigating Uber for allegedly operating a taxi service without the appropriate license (Yi Fan et al., 2017).

The Chinese use very vague, ambiguous language in the standards. This practice is assessed by experts as a way of reducing problems arising from relations with the World Trade Organization (WTO). At the same time, the ambiguities in the standards allow the Chinese government maximum flexibility and freedom to apply burdensome regulations to foreign entities, in particular when it considers it appropriate. Beijing may also rely on the fact that most standards are directive-based to avoid discretion. More than 1,000 Chinese standards (not only cyber security standards) previously submitted to the WTO were lowered from requirements for national standards to recommendations (in 2017 alone).

As the bilateral tensions between the US and China intensify, the standards associated with the new system of cyber security reviews are likely to be one of the first tools China can use to retaliate against US companies in a trade war. They offer the Chinese government the opportunity to delay the certification or issuance of licenses needed to gain market access, which may result in the closure of companies that may already have been "successful" in China. As a result, Beijing could use the standards to shift the basic requirements for foreign companies operating in China in a way that would have a long-term effect on short-term tensions in bilateral or multilateral relations.

2. Creating Cybersecurity Standards in China

In August 2016, a law on cybersecurity was published. A year before its entry into force, a group of three government agencies involved in the work on cybersecurity the standards issued an opinion which stressed the key role that standards should play in making President Xi Jinping's vision of building Chinese power in cyberspace a reality. The statement also describes how standards will support the implementation of the Cybersecurity Act (08.2016). In parallel, work continued and in November 2017, the National People's Congress issued a standardization law, which was last updated in 1988.[3] The new law codifies the recommendations of Chinese leaders to modernize China's standards system to keep pace with industrial and technological developments (USITC, 2010).

Chinese national standards are understood as policy instruments, and as a form of regulation that sets out requirements that

[3] Amendment of the law last updated in 1988.

can be used to control companies or used as a basis for testing and certification[4] (Ding, and Triolo, and Sacks, 2018). The Chinese government underlines its willingness to play a greater role in standard-setting in particular in areas such as 5G, which are international protocols or guidelines on design and interoperability. Some of these standards are required as a precondition for market access or sales - as indicated in public procurement lists. These standards have the letters "GB" at the front, which means "national standard" or "guobiao" (国 标). Others are recommended, but not formally binding, with the term "GB/T", which are "recommended" standards or guobiao/tuijian (国 标 / 推荐).

Even if standards are not officially required, companies may still be controlled by regulators and may require compliance with these standards in practice when:

- they are listed as public or government procurement requirements and
- when customers do not buy (do not conclude contracts) without a specific certificate.

The second requirement varies considerably depending on the sector or business segment. There are cases where contracts with customers are not finalized, because the product lacks a specific certificate. It is emphasized that failure to comply even with the recommended standards can result in high sales costs in China. Standards are also becoming required in conjunction with regulations that relate to these standards. The government can audit companies for standards, even if the standards are not officially required. As a result, compliance with the standards may be necessary to do business in China, even if the standards are only "recommended".

In China, all required standards must go through a process that will be officially approved. This is not an easy process in the Chinese political and legal bureaucracy. Moreover, Beijing must disclose the required national standards to the World Trade Organization (WTO) internationally. In fact, in 2017 the government downgraded more than 1,000 Chinese standards, not only from the set of cyber security standards Technical Committees ISO/TC260 (TC260) previously submitted to the WTO, from the required national standards to recommendations. As many as 396 mandatory national standards have been abolished and 1077 mandatory national standards have been converted into recommended national standards (Sacks, and Li, 2018).

The TC260 is not entitled to issue the required standards. There is, however, "circumvention" - the TC260 standards become de facto required when they are combined with specific legislation. In this way, they do not have to go through long agreements between the agencies. As a result, companies often have to apply even recommended standards to succeed on the Chinese market. In this way, they do not have to go through long agreements between the agencies. As a result, companies often have to apply even recommended standards to succeed in the Chinese market. Failure to do so can create enormous regulatory and political risks. This risk may increase if Beijing searches for ways to punish U.S. companies for the growing trade tensions in 2019 and 2020 (and perhaps even further into the future, with the unknown long-term effects of protectionism).

[4] Internationally, the Chinese government also stressed the importance of playing a greater role in standard setting (for example in areas such as 5G), which are international protocols or guidelines on design and interoperability. See: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table /online access [21.06.2020].

3. Foreign companies and the formation of Chinese cyber security standards

In 2016, China saw an important breakthrough in the field of standardization for foreign companies. To help develop China's cyber security standards, TC260 invited foreign participants to join the committee. This step was important in the end as foreign companies now take part in some discussions and are at least partly up to date. However, in general, their influence remains limited, it is local companies and the TC260 Secretariat who lead the core work[5] (Dou, and King, 2016). There are currently 16 foreign companies in these working groups that are members of the TC260. The structure of the foreign companies is shown in Figure 1.

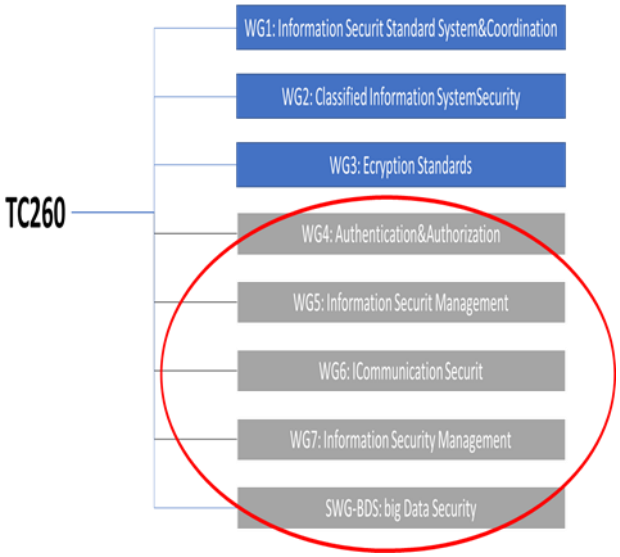

Figure 1. Structure of foreign companies in ISO/TC260. Own work.

According to participants, the Technical Committees ISO/ TC260 only accepts comments from foreign members that do not constitute real obstacles to the TC260. When comments from foreign members cause a conflict with the TC260's plans or interests of domestic companies, TC260 has applied a strategy of transferring the problem to one of the working groups closed to foreign participation. This approach was evident in the misunderstanding that emerged around the international standard interoperability initiative, the Trusted Platform Module (TPM). Chinese proprietary versions of the TPM standard required certain cryptographic algorithms for security tasks, such as verification, to be based on Chinese technology (USITC, 2010). When the WG7 voting which includes foreign members - stopped the initiative, TC260 addressed this problem in WG3 (encryption standards), which does not accept foreign members. The TC260 is likely to become even less sensitive to contributions from foreign members given the negative dynamics of cooperation between the US and China. Participation in the TC260 may help foreign companies gain political support from the government, but their presence may become increasingly symbolic.

4. Multi-level security program (MLPS)

The Ministry of Public Security has published a draft of a new version of the Multi-Level Protection Scheme (MLPS)[6] (called

[5] Microsoft has also been invited to join this committee to take an active part in developing the rules. The TC260 originally had 48 members and was expanded in January to 81 members, mainly Chinese officials and representatives of Chinese technology companies. The committee's seven working groups focus on encryption, large data and other cybersecurity issues. Earlier this month, 46 trade associations sent a joint letter to Chinese Prime Minister Li Keqiang, saying that the draft Cyber Security Bill, which will increase government monitoring and the data on fines will be stored locally, will "weaken security and separate China from the global digital economy" https://mspoweruser.com/china-invites-microsoft-to-join-technical-committee-260-tc260-to-draft-cybersecurity-rules/ online access [21.06.2020].

[6] The draft Regulation updating the original 2007 program is based on the new principles set out in the Cyber Security Act.

MLPS 2.0)[7]. According to the original MLPS plan, it ranks among the 1-5 ICT networks and systems that make up the Chinese Critical Information Infrastructures (CII) based on national security, and level 5 is considered to be the most sensitive. Level 3 or higher triggered a set of regulatory requirements for ICT products and services sold to this CII, including local IP products in China, shipping to government testing laboratories for certification and compliance with encryption rules prohibiting foreign encryption technology. A higher MLPS ranking meant that companies would be subject to enhanced monitoring by MLPS systems.

These factors have created barriers to market access as well as security risks for foreign companies. One of the most confusing but important issues in the new regulatory regime for cyber security is what exactly CII means. Under the Cyber Security Act, entities considered as CII have to face a package of new requirements. However, the government has not yet issued an official definition of CII or explained how these rules work with the existing MLPS. Currently, it seems that there are two parallel regulatory regimes for CII: one under the original MLPS and the other under the new regime set out in the Cyber Security Act. The government has not clarified the relationship between the two regulations; moreover, two government agencies, the Ministry of Public Security and Civil Aviation Administration of China (MPS and CAAC) have so-called overlapping jurisdiction over CII. MLPS 2.0 is likely to create greater regulatory control over foreign technology, although MLPS 2.0 seems to relax the original regime as it simplifies Chinese local IP requirements at level 3 and above. However, in parallel, MLPS 2.0 may increase control in other areas. For example, the document would potentially cover ICT products that were previously outside the scope of the MLPS, extending the program to cover all network operators, and not just those from CII or government agencies. According to MLPS 1.0, industries such as manufacturing or retail would not fall under the scope of the MLPS because they are not defined as CII. However, according to the draft MLPS 2.0 will cover any industry with an ICT infrastructure, through an unclear category called "network operators", which may include anyone using an ICT system. This seems to indicate that MLPS 2.0 also focuses on cloud computing, mobile internet and big data (Sacks, and Li, 2018).

Another challenge is that MLPS 2.0 may lower the threshold for the Grade 3 status, meaning that more companies (both Chinese and foreign) will be subject to enhanced monitoring by MPS, third-party certification and national encryption requirements.[8] In general, MLPS 2.0 is moving towards more government controls and audits instead of self-reporting by companies (Xiaomeng et.al., 2018). Standards play a key role in supporting the MLPS as they are used as a reference. They are used for testing, evaluation and classification against technical requirements at each level. Table 1 below illustrates the general structure of standards forming the existing MLPS (Sacks, and Li, 2018). The MLPS core standard ("Information Security Technology - The Basis for Cyber Security - Protection Classification: Part 1: General Security Requirements - The Basis for Other Standards") requires the provision of source code when a company at level 3 or above commissions the execution or development of software. MLPS standards related to access control may also favor local Chinese companies that have robust censorship (control) systems. One standard calls for censor-

[7] See: Seconded European Standardization Expert in China, https://www.sesec.eu/tag/cyber-security-digital-identity/, Ministry of Public Security Material on "Regulation of network security level protection (draft for comment)", Public Notice of Comments, http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html, [3.05.209].

[8] Expert analysis suggests that Chinese companies are likely to have fewer problems with these requirements in return: How Chinese Cybersecurity Standards Impact Doing Business in China.

ship and filtering of content at critical network nodes to control access. In this way, censorship of digital content could constitute a barrier to market access.

In a trade war scenario, the MLPS standards also provide Beijing with sufficient tools to take punitive measures against foreign companies on the basis of unclear approval rules. Network and system security management requires the authorization and approval of all connections to external networks, with regular inspections for violations. Other types of approvals that are not clear enough are needed in areas such as "design of security plan", which requires the approval of security plans and supporting documents.

Table 1.
General structure of standards forming the MLPS

Status of level	Requirements areas	Parts of Individual Standards
1	Standards on general requirements of multi-level protection scheme	INFORMATION SECURITY TECHNOLOGY **Baseline for Cybersecurity Classified Protection** Part 1: Security General Requirements Part 2: Security Special Requirements for Could Computing Part 3: Special Security Requirements for the Mobile Interconnection **General Requirements for Classified Protection of Cybersecurity Information Security Technology** Part 5: Special Security Requirements for Industrial Control System
2	Standards on design requirements of multilevel protection scheme	INFORMATION SECURITY TECHNOLOGY **Technical Requirements of security Design for Cybersecurity Classified Protection** Part 1: General Security Design Requirements
		Technical Requirements of Security Design for Network Security Classified Protection Part 2: Cloud Computing Security Requirements **Technical Requirements of Security Design for Network Security Classified Protection** Part 3: Security Requirements for the Mobile Internet Things Part 4: Security Requirements for Internet Things Part 5: Security Requirements of Industrial Control
3	Standards on testing and evaluation of multilevel protection scheme	**INFORMATION SECURITY TECHNOLOGY Evaluation Requirements for Cybersecurity Classified Protection** Part 1: Security General Requirements **Testing and Evaluation Requirements for Protection Network Security** Part 2: Testing and Evaluation Requirements Cloud Computing Security **Evaluation Requirements for Security Classified Protection** Part 3: Special Security Requirements for the Mobile Internet of Things Part 4: Special Security Requirements for Internet Things information Part 5: Industrial Control System Security Extension Requirements

Source: based on Introduction of the Framework of the Series of Standards on Cybersecurity Multi-Level Protection Scheme by Ma Li from MPS MLPS Evaluation Center. http://www.djbh.net/webdev/web/AcademicianColumnAction.do?p=getYszl&id=8a8182565deefd0d015e799ea2040094, in Sacks, and Li, 2018.

Foreign companies are not clear about the new rules, yet they are already under pressure from the Chinese government to meet increasingly onerous requirements.

Since the entry into force of the Cyber Security Act, much of the enforcement action against companies has focused on MLPS violations. This trend underlines the growing risk for companies related to the MLPS, officials are focusing in particular on this program to show progress in the implementation of the Cyber Security Act.

5. Cyber Protection of Critical Information Infrastructure (CII)

Under the Cyber Security Act, there is an intense debate on the relationship between the Multi-Level Protection Scheme (MLPS) and the new Critical Information Infrastructure (CII). The problem is unresolved as it is unknown which sectors are subject to CII. A characteristic feature of the Cyber Act is the burdensome requirements imposed on entities that are deemed to belong to critical infrastructure. Under the law, CII operators must only use network products and services that have undergone a vaguely defined review of the national security process (also known as a "black box" review). This includes the storage of certain data, regular security assessments and procedures, such as on-site testing.

In the draft regulation in May 2017, the scope for CII was presented. Under the Cyber Security Act, covering sectors such as energy, finance, transport and others, meeting the general criteria set out in Article 18, according to which: "The network infrastructure and information systems operated or managed by entities which, if destroyed, rendered inoperative or caused a data leak, could seriously harm national security, the national economy, the livelihoods of the population and the public interest shall be included in the scope of CII protection" (CII Security Protection Regulations, 2017). The development of Critical Information Infrastructure Protection Regulation standards is extremely slow.

The draft CII Protection Regulation suggests that standards will play an important role in clarifying unclear concepts, in particular as regards critical infrastructure itself. For example, the baseline standard issued on 11 June 2018 has little help in narrowing the definition of CII, using the expression "including but not limited to". Another standard contains a section that deals with the obligation to comply (base standard) with the MLPS for CII operators. It is concluded that some actors in CII areas, such as network infrastructure, big data, clouds and IoT, should take security measures according to the MLPS class. In pursuing the implementation of the MLPS 2.0 regime, it is noted that a competitive parallel CII protection regime is being developed. The draft CII Regulation refers to the regulatory authorities responsible for the different sectors, which should identify CII within their sector at all times.[9] As a result, foreign companies may be subject to uneven enforcement, as government stakeholders have wide discretionary powers to ring-fence competing regulatory systems and ensure priority.

6. Personal data and protection of sensitive data

The Cyber Security Act and its accompanying standard, known as the Personal Data Security Specification, set out the general principles for user consent and what companies should do to collect, store, process and transmit personal data. Beijing views the protection of personal data against fraud or

[9] "National sectoral controlling or supervision departments will, according to the CII identification guidelines, organize the identification of CII within those sectors and those areas, and report the identification results according to procedure," https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/ [21.06.2020].

misappropriation by companies or criminals as an essential element of cyber security.

However, this approach may imply a completely different understanding of data privacy from the Western concept and may be guided by different considerations (Xiaomeng, Manyi, Sacks, 2018). MLPS 2.0 even emphasizes the importance of protecting personal data through seven separate articles. Network operators who illegally allow a leak or sell or make it available without authorization will be punished. In practice, enforcement may be uneven and politically discredited because of unclear, undefined regulatory zones. The government has no other criteria for assessing how companies are to process personal data in addition to the specifications and unclear rules in the Cyber Security Act. In the future, the legislator may develop a separate national privacy law, but during this period the specification offers only general principles on this issue, which in effect means that it can be interpreted as required if officials want to enforce it.

The conflict between the specification and the Cyber Security Act also creates opportunities for law enforcement by ad hoc authorities. Regulators may penalize the company for collecting personal data without explicit consent (required under the Cyber Security Act), despite specifications allowing for implicit consent in some cases. That fact prevents transforming businesses and other forms of transactions from a centralized, human-based to a shared, algorithm-based trust model, which enables a new risk management paradigm (Drljevic et al., 2020).

7. Encryption

In accordance with generally applicable rules, the foremost short-term *technical* option recommended for ensuring data security and privacy is encryption (Schuster et al., 2017). In 2016, Beijing launched the world's first quantum satellite, “Micius”, which teleported pairs of entangled photons to Earth in 2017. This achievement will probably allow China to create the world's first quantum satellite network. In 2017, China also established the first long-distance quantum ground connection between Beijing and Shanghai, approximately 2000 kilometers long. In the future, it will probably be connected to the quantum satellite network.

These scientific achievements are groundbreaking initiatives that can protect Chinese government communications from foreign observations, at least until post-quantum cryptanalysis becomes a functional reality. For the development of quantum technologies, American companies from the private sector are important, including Google, IBM, Intel and Microsoft, which have been conducting quantum research for almost ten years (Kuczabski, 2019). In this context, it is not surprising that vague areas in the Chinese encryption regulatory system give authorities wide discretion to enforce requirements.

Moreover, the rules on what exactly foreign companies have to do to incorporate encryption into their products, as well as the use of encryption in their own communications, are currently undergoing major changes. The encryption bill has been under review for a long time. When enacted and enforced, the law may be interpreted as requiring the use of only pre-approved national encryption products (Luo, 2017). The grey market has been a concern for foreign industry for years, and the Chinese government considers that enforcement would be too costly for foreign companies, which have to stay in the market. The only exception in the current Regulation allows companies to apply for approval to use commercial encryption products produced abroad.

The draft law also includes unclear requirements for decryption in terms of national security (a provision also found in the Chinese Counter-Terrorism Act), on-site inspections to access data and seize equipment and an overview of national security for certain types of encryption products and services (Sacks, and Li, 2018). A statutory regulation would significantly strengthen the ex-

ecutive powers of the Chinese state cryptographic administration through enhanced government oversight and access to China's first uniform encryption system (Luo, 2017). As the rules for this new system are still being developed, they can easily become another retaliatory tool of the so-called 'backdoor' against foreign contraband. There are still serious gaps between the existing rules and the standards that create the aforementioned 'grey areas' that the authorities may interpret freely. For example, there are no standards that set out the details of the implementation of anti-terrorism legislation obliging companies to provide "technical assistance" to the government (which may mean decryption) to support national security investigations. There are also no standards related to encryption in the CII sectors - perhaps because the very meaning of CII is changing - even though it is a central point in the Cyber Security Act. Ambiguous rules in this area give authorities enough room for ad hoc enforcement of requirements and the possibility of wide discretion. Although many Chinese encryption standards adopt international standards, these include modifications to the use of algorithms approved by the Chinese encryption management departments. Examples include standards related to data integrity, digital signature and identity authentication. It is also important that government authorities have a wide discretion as to what they require companies to do in the process of performing an inspection related to encryption requirements.

With regard to the security standard, the test requirements for cryptographic modules state that "the burden of proof shall lie with the controlled company. If there is any uncertainty or ambiguity, inspectors should ask the inspected company to provide additional information" (ISO/IEC 24759 : 2017). Thus, encryption standards related to CII in particular will be an important area for observation in the coming years, especially as the Chinese administration is trying to define exactly what falls under this often-contested category.

8. Conclusion

Cyber security standards will be a key element in technical and commercial relations between China and abroad, especially in the US, as most US ICT companies are trying to enter the Chinese market or are already there. As the US takes an increasingly confrontational stance towards Beijing, the US must recognize the consequences of this as a cost to US companies, which concerns not only the form of reciprocal tariffs but also the perception and impediments to trade.

Currently, there are still many uncertainties. It is unclear what exactly the government is trying to protect under the hundreds of newly created standards. It is not clear how companies will be controlled. A positive development would be to make the processes to which foreign companies should adhere more transparent in order to avoid arbitrary audits. Undoubtedly, however, cyber security standards in China are an important and growing factor shaping the operating environment for foreign companies. This is important for any company that relies on an ICT infrastructure, including sectors dominated by public, government or private commercial entities. The standards provide authorities with "unclear" regulatory tools that can pose security risks, increase costs and underline the importance of total control.

These challenges will intensify as the trade war between the United States and China escalates, albeit in a difficult to quantify manner. The standards support new types of cyber-security reviews. Foreign companies need to have a clear picture of the layered and sometimes ambiguous regulatory nature to be able to use it to communicate their negotiating positions with Chinese partners and the government. Understanding the practical effects of standards, especially the avalanche of new cyber security standards can change the unfavorable status quo and can help prepare strategies for foreign companies. Unclear, and imprecise language in the standards and laws is often used to refer to different interests in the Chinese

system. Foreign companies and governments should recognize where debates take place and try to cooperate with interest groups similar to their own. Especially when the relationship between regulatory control and business interests in China is discussed, especially as many private Chinese companies expect to expand into global markets. The fact that Chinese global companies also benefit from Beijing's acceptance of more international standards is not insignificant.

In March 2019, annual meetings of the National Chinese People's Congress were held, which in the Chinese political system corresponds to parliament. These events are known in China as lianghui(会), i.e. "two meetings" because the People's Political Consultative Conference of China, which functions as an advisory body, also takes place simultaneously. The report that followed the deliberations contained references to the tense situation of the "trade war" with the USA and a call for internal consolidation and solidarity towards global challenges.

The set course of action is to counteract the deepening economic and social problems and to mitigate international tensions. In the Prime Minister of China's annual report, there is no reference to the strategy "Made in China 2025" although new regulations and laws serve to implement this strategy. The most important event of last year's National Chinese People's Congress, from the point of view of its international implications, was the announcement of a new law regulating foreign investments in China (Chinese Prime Minister Report, Xinhuanet, 2019). Although the new law appeared, its general nature may allow the government to continue its interference and unequal treatment of foreign entities in the Chinese market.

All political declarations and actions also affect standardization regulations. At the time of the detailed analysis from October 2018 to June 2019, the regulatory documents were not yet published, and the beginning of 2020s did not bring any changes in this respect.

References

1. *Critical Information Infrastructure Security Protection Regulations, July 2017.* http://www.cac.gov.cn/2017-07/11/m_1121294220.htm, *transl. by Graham Webster, Paul Triolo and Rogier Creemers* http://www.chinacopyrightandmedia. wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/, 21.06.2020.
2. Ding, J., and Triolo, P., and Sacks, S. (2018), *Chinese Interests Take a Big Seat at The AI Governance Table* http://www.newamerica.org/cybersecurity-initiative/ digichina / blog / chinese-interests-take-big-seat-ai-governance-table/, 21.06.2020.
3. Dou, E., and King, R. (2016), *China Sets New Tone in Drafting Cybersecurity Rules Allows Microsoft, Cisco, other foreign tech companies joint influential Technical Committee 260.* https://www.wsj.com/articles/china-moves-to-ease-foreign-concerns-on-cybersecurity-controls-1472132575, 21.06.2020.
4. Drljevic, N., and Aranda, A., and Stantchev V. (2020), Perspectives on risks and standards that affect the requirements engineering of blockchain technology, Computer Standards & Interfaces, Volume 69, pp. 10-17, DOI: 10.1016/j.csi.2019.103409.
5. ISO/IEC 24759:2017 (E), *Security Test Requirements for Cryptographic Modules* http://www.sis.se/api/document/preview/921732/, 21.06.2020.
6. Kezhi, Z. (2019) *Regulation of network security level protection Ministry of Public Security Material Report (Report No. n49)* Beijing: Public Notice of Comments.
7. Keqiang, L. (2019). *Highlights of 2019 Government Work Report* (Report No. 5.03.19). Beijing: China.org.cn.
8. Kuczabski, M. (2019). Środowisko przyszłej wojny stymulowane technologiami – wyzwania i zagrożenia. In R. Bielawski,

and J. Solarz, and D. Miszewski (Eds.), *Współczesne i przyszłe zagrożenia bezpieczeństwa cz. I* (pp. 175-196). Warszawa: Akademia Sztuki Wojennej.
9. Luo, Y. (2017), China Revises Proposals on Regulation of Commercial Encryption. Covington. https: //www.insideprivacy.com/, 21.06.2020.
10. Sacks, S., and Li, M. *How Chinese Cybersecurity Standards Impact Doing Business In China*. Retrieved from http://www.csis.org /analysis/how-chinese-cybersecurity-standards-impact-doing-business-china/, 21.06.2020.
11. Schuster, S., and Berg, M., and Larrucea X., and Slewe, T., and Kostic, P. (2017). Mass surveillance and technological policy options: Improving security of private communications. *Computer Standards & Interfaces*, *Volume 50*, pp. 76-82, DOI: 10.1016/j.csi.2016.09.011.
12. *USITC Publication 4199 (amended) November 2010*. http://www.usitc.gov /publications/332/pub4199.pdf, 21.06.2020.
13. Xiaomeng, L., and Triolo, P., and Samm, S., and Creemers, R., and Webster, G. *Progress, Pauses, and Power Shifts in China's Cybersecurity Law Regime*. http://www.newamerica.org/cybersecurity-initiative/digichina/blog/progress-pauses-power-shifts-chinas-cybersecurity-law-regime, 21.06.2020.
14. Xiaomeng, L., and Manyi, L., and Sacks S. (2018). *CSIS Report: What the Facebook Scandal Means in a Land without Facebook: A Look at China's Burgeoning Data Protection Regime (Report No. 04.25.2018)*. Washington: CSIS.
15. Xu, B. (2018). *SESEC IV China Cybersecurity Standardization* (*Report SESEC IV No. 1.2018)*. Beijing: China Cybersecurity News.
16. Yi Fan, Y., and Lu, M. C., and Luo, H. H., and Sung, Ch. (2017), Standardisation and Trade Barriere Issues Regarding the ICT Market in China: A Study of the Wi-Fi Industry, *Journal of Computers, Volume 28,* pp. 35-42 DOI: 10.3966/199115592017062803004.