before scholars can sufficiently understand what happens to law enforcement during a conflict, and how to make the best decisions regarding interventions or support.

Список використаних джерел

1. The US Army Stability Operations Field Manual 3–07 (The Stability Ops Manual), University of Michigan Press, Ann Arbor, 2009, para. 3–22.

2. Jones, S.G., Wilson, J.M., Rathmell, A., & Riley, K.J. (2005). Establishing law and order after conflict, Santa Monica, CA: RAND.

3. Kennedy D. Of War and Law, Princeton University Press, Princeton, 2006, 159 p.

4. Lutterbeck, D. (2004). Between police and military: The new security agenda and the rise of gendarmeries. *Cooperation and Conflict*. № 39(1). P. 45–68.

Литвинюк І.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Гіпська Т.**

CHINA'S CYBERSECURITY LAW AND ITS IMPACTS

China's Cybersecurity Law went into effect, marking an important milestone in China's efforts to create strict guidelines on cyber governance. Long before the Cybersecurity Law took effect, China had already made some efforts to strengthen information security. For example, a white paper titled The Internet in China, published in 2010, served as an early guide to China's policy on internet usage [1]. But the Cybersecurity Law marks a significant milestone in China's efforts to combat cybercrime.

Despite the Cybersecurity Law's passage and enactment, uncertainties still plague its introduction. Because of ambiguous requirements and broadly defined terminology, some enterprises are concerned about the law's potential impact on their operations in China, while others worry that it will create trade barriers to foreign companies in the Chinese market.

Consisting of 79 articles in seven chapters, the Cybersecurity Law is exceptionally wide in scope, containing an overarching framework targeting the regulation of internet security, protection of private and sensitive information, and safeguards for national cyberspace sovereignty and security. Similar to some of the most commonly used cybersecurity standards, such as the Cybersecurity Framework of the National Institute of Standards and Technology (NIST) and ISO 27000-27001, the Cybersecurity Law emphasizes requirements for network products, services, operations and information security, as well as monitoring, early detection, emergency response and reporting. On the topic of protection of data privacy, the Cybersecurity Law is similar to data-privacy laws and regulations in other

jurisdictions. However, the requirements related to national cyberspace sovereignty and security are more distinct [4].

The Cybersecurity Law expressly applies to network operators and critical information infrastructure (CII) operators, as the terms for these entities are repeatedly mentioned in the law. «Network operator», as defined in the appendix to the Cybersecurity Law, could be applicable to almost all businesses in China that own or administer their networks. Due to the loosely defined terms, however, the Cybersecurity Law may be interpreted to encompass a wide set of industries apart from traditional information technology, internet service providers and telecommunications companies.

Therefore, it is safe to assume that any company (regardless of size and domestic or multinational extent) operating its network – including websites and internal and external networks – to conduct business, provide a service or collect data in China could very likely be in scope [3].

Although the CAC has yet to issue further guidance on CIIs, it has incorporated a wide range of industries, including but not limited to communications, information services, energy, transportation, utility, financial services, public services and government services. In general, the requirements for network operators and CIIs are similar in terms of their objectives, but the requirements for CIIs are more stringent.

Four out of the seven chapters in the Cybersecurity Law outline its major requirements:

1. Network: policies and procedures, network products and services, security assessment and information storage
2. Information Security: protection of private information and collection, usage and distribution of information
3. Monitor and response: live monitoring, comprehensive incident response, incident drill and risk assessment
4. Regulatory penalties: removal from office and maximum fine RMB 1 million, plus suspension of business and revocation of licenses.

Shortly after the Cybersecurity Law went into effect, regulators leveraged the new law in their investigations across various industries and enterprises. Among those under current investigation according to the Cybersecurity Law are some of China's biggest social media platforms: Tencent, Baidu and Sina Weibo. The three internet giants are under investigation for potential violations of the Cybersecurity Law – specifically, their potential failure to control users who have posted inappropriate content. Such investigations appear to be related to national cyberspace sovereignty and security. Other reported cases for different causes (e.g., articles 21, 24 and 47) have resulted in monetary penalties or warnings to remediate those violations within a given period.

Among the actions that companies should consider taking as they determine how to comply with the Cybersecurity Law include the following:

- Take stock of how information is collected, processed and stored, including private sensitive information.

- Assess cybersecurity and privacy risks and threats in order to focus cybersecurity efforts on the most critical risks and threats.
- Strengthen overall security governance, especially security policies and procedures.
- Evaluate business processes to ensure that proper controls are in place for the collection, use and storage of private information.
- Develop clear roles and responsibilities for cybersecurity and privacy management.
- Set up a security and privacy incident monitoring system and appropriate reporting mechanisms.
- Execute periodic cybersecurity assessments.
- Ensure proper safeguards of private and important information transmitted outside of China's borders (including security assessment).
- Design a proper security incident response plan and perform periodic drills [4].

Список використаних джерел

1. The Internet in China, People's Daily Online, June 2010. URL: http://en.people.cn/90001/90776/90785/7017177.html.
2. Cyberspace Administration of China, Draft Security Assessment Measures for Cross-Border Transfer of Private Information and Important Data (in Chinese). URL: http://www.cac.gov.cn/2017-04/11/c_1120785691.htm.
3. Hong Kong's Personal Data (Privacy) Ordinance. URL: https://www.doj.gov.hk/eng/blis_decommission/index.html/blis_pdf.nsf/CurAllEngDoc.
4. China's Cybersecurity Law and its Impacts - Key Requirements Businesses Need to Understand to Ensure Compliance. URL: https://www.protiviti.com/HK-en/insights/china-cybersecurity-law-and-impacts.

Лобас В.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Сторожук О.**

LINGUISTICS AND LAW IN THE SECURITY SPHERE: FOREIGN EXPERIENCE

Linguistics and law are related to conservation issues national security, and when this happens, the inclusion of security brings certain ideologies into politics. One argument often found in security-focused linguistic politics is the idea that security requires society as a whole to have an understanding and knowledge of those nations or other groups that constitute possible security threats and language education is seen as a way to develop such understanding and knowledge.

There are general issues related to language education policy related to national security, as well as specific policy initiatives at certain historical