participation of members of the public in the administration of justice is a form of exercising the sovereignty of the people in the functioning of this important branch of government.

Список використаних джерел

1. Щерба В. М. Суд присяжних в Україні: окремі питання становлення та розвитку / В. М. Щерба // Порівняльно-аналітичне право. – 2013.

2. Соловей В. Переваги та недоліки створення інституту суду присяжних в Україні / В. Соловей // Аналітика. – 2012.

3. Закон України «Про судоустрій і статус суддів»

Дмитренко Д.,
студент Національної академії внутрішніх справ
Консультант з мови: **Могилевська В.А.**

КОМП'ЮТЕРНА БЕЗПЕКА: ДОСВІД БОРОТЬБИ У КНР
CYBER SECURITY: CHINESE EXPERIENCE

China is resolutely moving forward with development of its own IT industry. It is also isolating itself from international IT technology. By exercising control over major state-run businesses, the PRC is also maintaining its sovereign position in the IT sector. The government supports the international expansion and sales endeavors of Chinese IT companies – the 'national champions'.

The main tasks of this thesis are to analyze the following points: inadequate quality regulations in China are posing a threat to IT security; censorship and restrictions on internet connections place constraints on China as a business location; concerns about IT espionage and theft of company secrets driving international businesses to transfer personnel or entire departments to other Asian countries; Chinese internet users are threatened by a shadow IT economy; illegal programs are often installed on computers and are not provided with security updates; hackers can gain access to these unprotected computers and use them as a base for worldwide attacks. Instead of insistently calling for fundamental changes in Chinese internet policy, the Federal Government of Germany ought to negotiate specific improvements for German businesses, for example in terms of market access or protection of intellectual property rights.

An alliance of fifteen private Chinese IT manufacturers was founded in the Beijing district of Zhongguancun (中关 村), the Chinese equivalent of Silicon Valley. They stepped up endeavors to develop a Chinese operating system based on Linux that would run on government computers and the computers of security relevant businesses such as banks. By taking this step, Beijing hopes to gain protection from espionage from the USA and demonstrate the innovative power of the Chinese IT economy. [1] In spite of the rampant growth of its IT industry, China is still dependent upon foreign technology at the moment. According to Xinhua, the state news agency, ninety per cent of its microchips and sixty five per cent of its firewall products originated in other countries in 2012, primarily the US.[2] The government views foreign technology as a potential threat to national security. Covertly installed back doors enable surveillance of computers and networks, for example. Therefore, stringent constraints on the use of foreign IT products are already in place in areas critical to security. At the same time, sealing the domestic market off from external influence is intended to foster the development of industrial and innovation policies in China: the government in Beijing wants to strengthen the competitiveness of domestic IT companies. [3] The Chinese government has succeeded in promoting a dynamic IT industry with robust private companies while retaining control over the sector.

Isolationism and protectionism lead to another problem for Chinese IT companies: the obligation to censor the internet. Not only does censorship affect freedom of speech, but it also impacts the entire economy. Operating a social network in China is expensive. The State Council Internet Information Office (国家互联网信息办公室) places tight restrictions on information from the internet. To comply with these controls, ISPs are required to employ two to three censors per 50,000 users.[4] For Sina Weibo, with around 300 million users, this means employing 15,000 people for the sole purpose of monitoring the content of the web pages the users invoke – a huge undertaking with considerable financial repercussions. By comparison, the sector’s leader, Facebook, employs a total of only 8,500 staff worldwide. [5] Internet censorship also impairs the development of software and apps. Google and other ISPs grant developers global access to program libraries and web fonts free of charge. This service helps programmers save time and money. Since data in China is blocked by internet censorship, programmers there have to redevelop the data themselves.

Cyber security – a key location factor for foreign companies, but censorship and cyber attacks hurt business. Foreign companies in China must comply with ever more stringent regulations in the IT sector, impeding their ability to protect business secrets and hindering international cooperation. China represents the largest market in the world for Apple; the iPhone is very popular there. Lately it became known that hackers had targeted data transmission to the company's iCloud service. Due to the complexity of the hack, IT experts suspect that the Chinese government was behind the attack or at least knew about it. However, just a few days later, Apple's chief executive, Tim Cook, went to Beijing and held discussions with key decision-makers at party headquarters, Zhongnanhai (中南海). This shows that Beijing has to deal with security reservations on the part of large Western companies in spite of its market power.[6] Other companies also feel the impact of cyber attacks and censorship. International collaboration with services such as Gmail, Google Docs or Dropbox is becoming increasingly dysfunctional. The same applies for virtual private networks (VPNs), with which users seek protection for information and business secrets.

Western suppliers on the Chinese market have to conform to parallel Chinese IT standards. The Chinese wireless LAN technology called WAPI Figure('WLAN Authentication and Privacy Infrastructure') is one example. Even though WPA2 encryption has become the international standard, China has deliberately gone separate ways since 2003. For foreign suppliers of routers and WLAN-compatible devices, this means they have to share their source code with one of eleven licensed Chinese IT companies and contribute to the development of the WAPI standard. Due to insufficient WAPI support, Apple was not allowed to sell the first version of its iPhone in China in 2010 until adjustments were made. Disputes between Chinese and Western IT companies over their market share and market access are rather secondary to the security of users in China. For them, it is imperative that they are able to shop securely online and that their computers cannot be hacked. There are major electronics markets in cities such as Shenzhen and Hong Kong. Visitors have a wide selection of software and hardware products to choose from, many of which are manufactured and distributed illegally, however. Software piracy is clearly harmful to Western manufacturers: according to their own figures, they lose billions in license fees. Former Microsoft head Steve Ballmer, for instance, once indicated that ninety per cent of the company's products in China were being used illegally.[7] What's more, pirated copies generally do not include any security updates, a fact that is especially problematical in key components such as operating systems. Susceptible devices are not only a security hazard for their users, they also threaten network security worldwide: if security gaps are not closed up, criminals can gain access to users' devices and employ these as 'zombie computers' in botnets. This enables them to steal additional access data from users or attack websites or network infrastructure. Illegally sold operating systems also frequently contain deliberately embedded viruses. Criminal hackers are a menace to the well-being and privacy of Chinese internet users. Illegal services are unabashedly offered in public forums, so there is obviously little fear of prosecution.

The ways and means with which illegal services are offered and advertised in China differ fundamentally from those in Western countries. While trade in stolen passwords or credit-card data generally runs via encrypted networks, Chinese hackers co-ordinate their illegal activities in open chat groups in QQ or forums run by Baidu. Criminals can purchase access to servers with which they can infect users with malware or send spam messages. Custom-made Trojan horses or creation of counterfeit sign-in pages for banks and social networks are also available – thus, PCs and smartphones can also be spied on.

China's steady expansion of its own IT industry and growing isolation from foreign products has been felt keenly by international manufacturers. Germany's cyber policy towards China must be prepared for conflict. In the long run, China will not agree to become integrated into a cyber-security system defined by Western concepts. In fact, Beijing is already working with other newly industrialized countries on parallel standards for internet governance, which has been dominated by the West up to now. As far as IT services and products for high-tech sectors are concerned – for instance in the area of Industry 4.0 and specialized business software – German companies can rely on their competitiveness in the face of Chinese rivals. The question is, for how much longer? It would therefore be wise for Germany to pursue a policy that has already proved to be effective in other fields. Instead of working towards fundamental change in Chinese cyber security, the Federal Government of Germany should focus on pragmatic goals that are attainable in practice. After all, there are enough urgent topics to be dealt with as it is, such as better protection of intellectual property or secure market access for German companies.

Список використаних джерел

1. Zhang, Yu (2018). 'Homegrown developers look to unseat Microsoft's dominant OS http://www.globaltimes.cn/content/887716.shtml

2. Zhangwei 张卫 (2017). '信息安全的机遇与挑战'(Opportunities and Challenges of Information Security) http://news.sohu.com/20120416/n340660958.shtm

3. Zhonghua renmin gongheguo guowuyuan 中华人民共和国国务院 (2017). '国务院出台意见推进信息化发展切实保障信息安 全' (The State Council publishes a document on promoting the development of informatization and for the protection of cyber security). http://politics.gmw.cn/201207/17/content_4571519.htm.

4. King, Gary, Pan, Jennifer and Roberts, Margaret E. (2016). 'Reverse-engineering censorship in China: Randomized experimentation and participant observation', Science 345 (6199): 1–10.

5. Facebook Newsroom (2016). Company Info. http://newsroom.fb.com/company-info

6. Lovejoy, Ben (2018). 'Tim Cook meets with Chinese vice premier in Beijing following iCloud phishing attack', http://www.techgreatest.com/apple-news/tim-cook-meets-withchinese-vice-premier-in-beijing-following-icloud-phishingattack/.

7. Brodkin, Jon (2011). 'Ballmer to Hu: 90% of Microsoft customers in China using pirated software', http://www.networkworld.com/article/2199038/software/ballmer-to-hu--90--of-microsoft-customers-in-china-using-piratedsoftware.html

Добридень Г.,
курсант Національної академії внутрішніх справ
Консультант з мови: **Шемякіна Н.В.**

LA LUTTE CONTRE LA CYBERCRIMINALITÉ EN FRANCE

En droit français, la cybercriminalité est définie comme l'ensemble des infractions pénales qui sont commises via les réseaux informatiques, notamment, sur le réseau Internet. [1]

La cybercriminalité se développe considérablement dans le monde de la technologie. Les criminels du World Wide Web exploitent les informations personnelles des internautes à leur avantage. Ils utilisent allègrement le dark web pour acheter et vendre des produits et des services illégaux. Ils réussissent même à avoir accès à des informations classifiées du gouvernement.[2,5]

Il faut souligner que les premiers cas de cybercriminalité ont eu lieu avant même qu'Internet n'existe et étaient liés … au vol de données. Les ordinateurs, les réseaux informatiques et Internet ont été conçus pour la création, le stockage et le transfert d'informations gouvernementales et de données d'entreprise, des informations très utiles pour les individus ayant de bonnes intentions. La création de méthodes numérisées peut avoir aidé l'humanité à se développer au 21ème siècle, mais cela a produit les mêmes effets pour les criminels. Ces derniers veulent ce que nous avons et plus nous essayons de dissimuler ces informations, de les rendre compliquées à récupérer et à exploiter et plus ils ont envie d'y accéder. Pas forcément pour en tirer profit, parfois juste pour prouver qu'ils peuvent y avoir accès. [2,5]

La cybercriminalité se divise en trois grandes catégories : la cybercriminalité individuelle, la cybercriminalité contre la propriété et la cybercriminalité gouvernementale. Les types de méthodes utilisées et les niveaux de difficulté varient selon la catégorie. Cela signifie que la cybercriminalité a instauré une menace majeure pour les utilisateurs