ПОЛІТИЧНИЙ ТА СОЦІАЛЬНО-ЕКОНОМІЧНИЙ РОЗВИТОК КИТАЮ

ISSN 2616-7328 (Online), ISSN 2409-904X (Print)
Kitaêznavčì doslìdžennâ, 2022, No. 1, pp. 5–21
DOI: https://doi.org/10.51198/chinesest2022.01.005

UDC 355.45:004.7[510]

CHINA'S NATIONAL CYBERSECURITY POLICY: INSTITUTIONAL PRESSURES

Yu. H. Shevchenko
Master's student, Political Science
Shanghai Jiao Tong University, School of International and Public Affairs
800 Dongchuan RD. Minhang District, Shanghai, China, 200240
shevchenkoyuliya98@gmail.com

The article studies the driving factors behind the formation of China's national cybersecurity policy through the application of the institutional theory. The institutionalization of China's cyber governance is explored by evaluating the impact of coercive, mimetic and normative pressures, originally suggested by DiMaggio and Powell in the organizational theory. The article provides an overview of China's reforms in the Internet field, the domestic institutional framework regulating cyberspace in China, and a review of the documents passed since 2014. The factor of US threat is evaluated as a coercive force, which boosted proactive reforms of China's national cybersecurity policy. New initiatives in cyber governance realm proposed by Western states push Chinese officials to encourage local response, often mirroring the actions of other states and adapting them to national needs. Thus, the Cybersecurity Law of 2017 and the Personal Information Protection Laws of 2021 are compared to the General Data Protection Regulation adopted in the EU. The introduction of domestic legal and normative reforms and promotion of the "cyber sovereignty" doctrine by the Chinese government is studied along with the existing regulations and norms in the cyber governance and contrasted with the position of the Western states. In China, the government is the major driving force behind the formation of national cybersecurity policy reforms and since 2014 the agenda in the regulation of Internet space has been clearly defined both domestically and internationally. China's intention to extend its position in global governance is based on the belief that it should shift from being a "rule taker" to a "rule creator". However, China still has a long way to go to align the actual readiness of private enterprises and the society with the policy goals.

Keywords: cybersecurity, cyber sovereignty, institutional pressures, Cyberspace Administration of China, Internet governance.

НАЦІОНАЛЬНА ПОЛІТИКА КІБЕРБЕЗПЕКИ КИТАЮ: ІНСТИТУЦІОНАЛЬНИЙ ТИСК

Ю. Г. Шевченко

У статті досліджуються рушійні чинники формування національної політики кібербезпеки Китаю через застосування інституційної теорії. Інституціоналізація кіберуправління в Китаї досліджується шляхом оцінки впливу примусового, міметичного та нормативного тиску, спочатку запропонованого Ді Маджіо та Пауеллом в організаційній теорії. У статті подано огляд реформ Китаю у сфері Інтернету, внутрішньої інституційної бази, що регулює кіберпростір у Китаї, та огляд документів, прийнятих з 2014 року. Фактор загрози США оцінюється як примусова сила, яка стимулювала активні реформи Китаю у сфері національної політики кібербезпеки. Нові ініціативи у сфері кіберурядування, запропоновані західними державами, спонукають китайських чиновників заохочувати місцеву реакцію, часто відображаючи дії інших держав і адаптуючи їх до національних потреб. Так, Закон про кібербезпеку 2017 року та Закон про захист персональної інформації 2021 року порівнюються із Загальним регламентом про захист даних, прийнятим в ЄС. Запровадження вітчизняних правових та нормативних реформ та просування доктрини "кіберсуверенітету" урядом Китаю досліджується поряд з наявними правилами та нормами в кіберурядуванні та протиставлено позиції західних держав. У Китаї уряд є основною рушійною силою формування національних реформ політики кібербезпеки, і з 2014 року порядок денний у регулюванні інтернет-простору чітко визначений як на внутрішньому, так і на міжнародному рівні. Намір Китаю розширити свої позиції в глобальному управлінні ґрунтується на переконанні, що він повинен перейти від "приймача правил" до "творця правил". Проте у Китаю ще багато попереду, щоб узгодити реальну готовність приватних підприємств і суспільства з цілями політики.

Ключові слова: кібербезпека, кіберсуверенітет, інституційний тиск, Адміністрація кіберпростору Китаю, управління Інтернетом.

Introduction. Cyberspace is consistently growing. Therefore, countries all around the globe strive to establish resilient national frameworks for cybersecurity. It is not an easy task, since the field is evolving at an unprecedented speed with countless computers, electronic devices, servers, routers, and fiber optic cables creating an interconnected cyberspace and being under permanent risk of getting disrupted or hacked. Meanwhile, cybersecurity is integral to economic prosperity, which is why countries need to secure national banking systems, online services, administration and government databases, etc. to support the nations' economic growth [Balke 2018]. As more resources are invested in the development of cutting-edge Internet technologies, the security considerations around those are now becoming a priority for central governments and respective institutions responsible for civil and military security.

Each state develops its national cybersecurity based on different incentive and pursues a varied strategy. According to the China Internet Network Information Center (CNNIC), at the end of December 2020, the country could boast 989 million internet users [Ghosh 2021]. As China has been getting increasingly dependent on various Internet assets, the Chinese authorities have been reacting accordingly. Over the span of the last decades, China's government significantly increased its emphasis on cyber security measures, while taking advantage of the opportunities that the world wide web provides [Raud 2016, *5*].

While China's national cybersecurity framework has been explored by both by Western and domestic researchers, the avid interest in the variables affecting the process of cybergovernance and policy fromation is still present. The case of China is particularly worth exploring due to the progressive and fast-paced development of national cybercapabilities, active involvement in the formation of international 5G standard-setting, pursuit by the government of "cyber sovereignty" principles and on-going "strategic competition" with the US.

Solid theoretical approaches to comprehend the institutionalization of cyber governance structures both internationally and domestically are still in embryotic phase. A major reason for this is that cybersecurity is an interdisciplinary field, which rapidly evolves at a difference pace in different states. The largest and most comprehensive annual review of cybersecurity capabilities for the majority of countries is conducted by the UN's International Telecommunications Union (ITU)'s Global Cybersecurity Index (GCI). According to GCI, China went through gradual yet quick-paced growth of national Internet security landscape starting from 2014 [Table 1]. However, the report lacks the review of offensive capabilities. The qualitative assessment of the International Institute for Strategic Studies as a part of the "Cyber Power Project" views China as a second-tier cyber power, with strong chances of joining the US in the first tier soon [The International Institute for Strategic Studies 2021]. Large-N study proposed by the Harvard Belfer Center in 2020 introduces the National Cyber Power Index (NCPI), which ranks China as the second cyber power right after the US, leaving all other states behind [Voo… 2020].

In-depth research on China's cyber capabilities has been conducted by such researches as Jon R. Lindsay [2015], Cheung Tai Ming [2015], Xu Longdi [2014], Lu Chuanying [2016; 2020], Raud Mikk [2016] and Greg Austin [2018]. While providing significant contribution to the study of the topic, their research can be further strengthened by new application of underexplored theoretical frameworks and exploration of the roles played by institutional variables in the formation of China's national cybersecurity policy. In the present article the formation and development of China's national cybersecurity policy and the cyber-governance structure are explored through the perspective of the institutional theory, which prescribes that coercive, mimetic and normative pressures have an impact on institutional isomorphism.

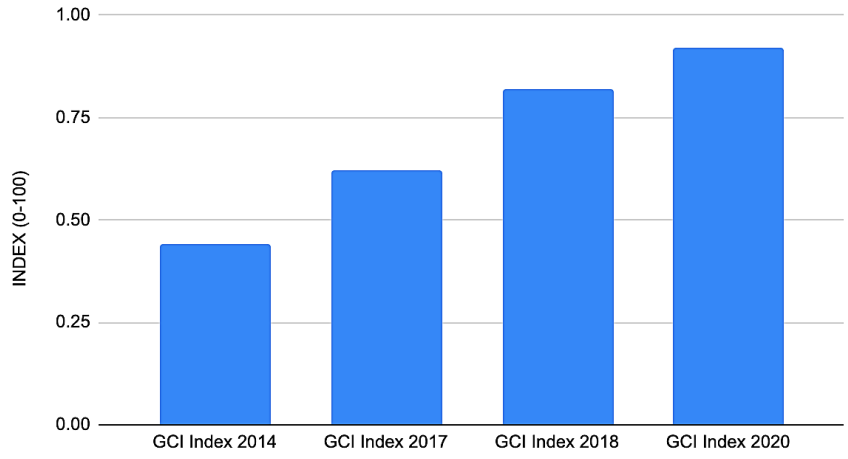

Table 1. China in the ITU's Global Cybersecurity Index [GCI]

Source: [ITU]

Theoretical Framework. In this research, the institutional theory is applied to analyze the drivers behind the formation of the China's national cybersecurity institutional landscape. The theory was introduced in the late 1970s by John Meyer and Brian Rowan and since then it has become a popular perspective within management theory because of its ability to explain organizational behaviors that defy economic rationality. The general idea behind the theory is that the institutional environment can strongly influence the development of formal structures in an organization. As a result, for a while, it became a dominant approach specifically in organization studies.

When applying institutional theory in political discourse, it is important first to explore the concept of "institution". Jepperson [1991, *150*] writes that "institutions represent a social order or pattern that has attained a certain state or property". Based on this idea, institutions are not reproduced by "action", rather by reproductive procedures which sustain this pattern. Scott [1995, *33*] states that "institutions consist of cognitive, normative and regulative structures and activities that provide stability and meaning to social behavior." Peters [2019, *157*] suggests that both definitions are too broad and their drawback is that they do not differentiate institutions from other forms of organization or social structure. Therefore, he suggests making some differentiation between institutions and organizations. Peters [2019, *149–156*] also discusses different contemporary approaches to institutions within sociology: the population ecology approach, institutionalization and isomorphism, formation of organizational archetypes, discursive institutionalism and institutional logics.

The institutionalization and isomorphism's main question is "Why do relatively similar forms of institutions emerge in very different social and political settings?". DiMaggio & Powell [1991, *64*] argue that bureaucratization and other forms of homogenization emerge out of the structuration of organizational fields. In 1983, after looking for an explanation of why organizations in a certain field tend to look and act similarly, DiMaggio & Powell [1991, *68*]. Identified and explained three "pressures" that determine how adopted behaviors and practices become isomorphically accepted by the organization field as a whole. These three forces are: coercive, normative, and mimetic.

Originally, the demands from entities that have resources on which an organization relies are referred to as coercive isomorphism. In organizational theory, professional norms and practices are referred to as normative isomorphism. DiMaggio & Powell [1983, *152*] described it as the "collective struggle of members of an occupation to define the conditions and methods of their work". When an organization is undecided on which strategy to follow, mimetic isomorphism occurs due to the practice of copying successful organizations in their practices [DiMaggio & Powell 1991, *68–73*; Safa, Von Solms and Furnell 2016; Daddi… 2019].

By examining and measuring the organizational field around these three pressures it is possible to understand convergence on homogenized practices and accepted behaviors in organizations. So coercive, normative, and mimetic pressures can guide the institutionalization of organizations. The usage of these three pressures has been already widely applied in the study of isomorphism of ICT practices in organizations [Teo, Wei and Benbasat 2003; Liang… 2007; Daddi… 2019]. Organizations are subject to these pressures because of the need to obtain legitimacy in the eyes of external constituents [e. g. clients, trade associations, regulatory actors, etc.] in order to profitably pursue their business objectives [Daddi… 2019].

Björck [2004] is among the first to present arguments in favour of deploying institutional theory in Information System/ Information Technology (IS/IT) security research by studying the adoption of ICT regulations in organizations. Hovav & D'Arcy [2012] call for applying institutional theory to understand better compliance of organizations with information security regulations, standards, and policies. Teo, Wei, and Benbasat [2003] demonstrated that three institutional pressures can potentially impact organizations' intention to adopt interorganizational linkages. Liang et al. [2007] found that these institutional forces can influence the beliefs and participation of top management in assimilation of enterprise resource planning (ERP) systems. Their theoretical framework is grounded in the proposition that institutional forces affect organizational behavior after being mediated by the top management. Zheng, Huang, Chen & Zhang (2013) studied e-governance in public administration organizations and explored the varying degree of mimetic, normative and coercive pressures in this context. Daddi et al. [2019] test their hypotheses that coercive pressures are negatively related to the change in managerial sensitivity, while normative and mimetic pressures are positively related to it. Jeyaraj & Zadeh [2020] examine how organizational cybersecurity responses become isomorphic over time. Drawing on institutional theory, this study theorizes that mimetic pressures, normative pressures, and coercive pressures impact cybersecurity responses. Their findings show that mimetic pressures were significant over time while coercive pressures were significant in the near-term and normative pressures were significant in the long-term.

Singh & Alshammari [2020] claim that despite multiple applications of institutional theory in the ICT field in general, there are scant attempts to apply it in the critical area of cybersecurity. The authors select this theory due to its scope and its lack of application to the area of cybersecurity in order to study the case of Saudi Arabia. Also, the authors make a suggestion that the concept of three pressures could be used at the level of the country, instead of an organizational or individual level. This idea can thus be applied to the analysis of the broad variety of factors (e. g. internal / external or governmental / private sector) influencing the institutionalization of cybersecurity in countries around the world.

Thus, in the following section the formation of China's national cybersecurity framework is explored based on the three institutional pressures – coercive, mimetic and normative.

China's National Cybersecurity Policy

General overview. China enjoys a great level of self-reliance in space-based intelligence, surveillance, and reconnaissance (ISR) capabilities, and invests heavily in R&D associated with quantum technologies and AI. These initiatives are strongly supported on the government level. It can be seen that in China the government serves as a locomotive of main reforms in the cybersecurity policy, while the private sector still needs some time to catch up with the strategic goals outlined in the normative documents. Institutional rearrangement pioneered by Xi's administration paved the way to the efficient functioning of the government apparatus both in civil and military security domains.

Many enterprises in China have gradually become aware of the impact of network security on their potential for survival. As a result, technology and management strategies are developing rapidly. China also holds a world-leading position in e-commerce, which

accounts for over one-third of the country's total GDP and saw a 10 percent growth on a yearly basis to over 39 trillion RMB (US$6 trillion) in 2020 [The State Council 2021]. However, ongoing dependence on foreign vendors for major cyber-technologies, e. g. Microsoft, Cisco, Qualcomm and IBM, is still a shortcoming despite the "Made in China 2025" strategy [The International Institute for Strategic Studies 2021; Austin 2018]. China also has not created a solid alternative operating system to replace Windows or macOS. Cyber-security research and education in China is still developing.

The Chinese state's approach to cybersecurity is grounded in "information security" and social stability. For Chinese authorities, public order in cyberspace is intricately connected to public order in physical space [Jiang 2020, *13*]. Many non-authoritative civilian and military Chinese sources acknowledge that back in 2013 China's cyberinfrastructure and internet laws were vulnerable and weak compared to those of other countries. Non-authoritative sources repeatedly asserted that China was highly vulnerable to cyberattacks because it relies primarily on developed countries – and especially the United States – for core network technologies [Swaine 2013].

On the legal and conceptual side, China's intention of becoming a cyber power was reflected in its military strategy released in 2015 and further described in the first formal national cybesecurity strategy in 2016. This document was passed quite timely, because the Chinese government has also declared high aspirations for the domestic production of the fundamental internet technologies it relies on, seeking to become a world leader in such technologies by 2030 [The International Institute for Strategic Studies 2021, *89*]. The next major milestone was the enactment of the Cybersecurity Law in 2017, which became a legal framework for dealing with cybersecurity and data regulation that aligns these piecemeal rules [Cyber Magazine 2021]. It was then followed by the adoption of the Data Security Law and Personal Information Protection Law in 2021.

The main body in charge of Internet regulations is the Cyberspace Administration of China (CAC). On the civilian side, CAC has become the focal point of all cyberspace policy, although powerful independent nodes remain – such as the Ministry of Public Security (MPS), the Ministry of State Security (MSS) and the Ministry of Industry and Information Technology. According to Austin [2018], the distinction of responsibilities between these bureaus is often very vague. In the military field, the Strategic Support Force (SSF) was established in 2015. It encompasses most of PLA's cyber capabilities. However, similarly, as with the civil structures, SSF was formed based on the restructuring of existing units under a consolidated command structure [The International Institute for Strategic Studies 2021]. It reports directly to the Central Military Commission and consolidates cyber-related operations under one roof, while previously these functions were performed by the different PLA units.

Today China actively participates in cyberspace governance mechanisms at the multilateral and international levels, whether it is the Group of Governmental Experts on Information Security under the UN framework, the International Telecommunication Union, the World Summit on the Information Society, the Internet Governance Forum, or outside the UN framework [Lu 2016]. Chinese officials are determined to influence cyberspace and its guiding principles. For example, the Chinese representative's formal speech at the Budapest Conference on Cyberspace in 2012 contained remarks criticizing the US for militarizing cyberspace and unjustly dividing cyber resources among mainly developed governments to retain its dominance [Raud 2016, *8*]. This is why China is determined to play a critical role in developing an alternative common and inclusive

global Internet governance model that more equally redistributes digital resources and governance rights as an opposition to Western initiatives. The International Strategy of Cooperation on Cyberspace issued by the Ministry of Foreign Affairs and the Cyberspace Administration of China in 2017 is also illustrative of this standpoint. Chapter 2 of the document calls for rejecting the Cold War mentality, zero-sum game and double standards, and upholding peace through cooperation [Xinhua 2017].

Pressures

Coercive. Coercive isomorphism is originally defined as the pressures from entities that have resources on which an organization depends [DiMaggio & Powell 1991, *68–73*]. If applied to the context of international relations, coercive pressure can mean factors which stem from angst caused by dependence on other governments or national incapability to provide the necessary degree of security, i.e. dependence on external circumstances.

Many researchers draw attention to potential external threats to China's network security as the key factors leading to the formation of modern cybersecurity framework. To a large extent, the spike in China's activization of national efforts in establishing cybersecurity resilience is attributed to the rising concerns about cyber military and espionage activities of the United States. This involves witnessing Washington's offensive capabilities after Stuxnet attack on Iran, revelations made by Edward Snowden in June 2013 [Swaine 2013; Lu 2016; Austin 2018; Jiang 2020], as well as increasing effort in the United States to develop its cyber military power [Austin 2018, *9*].

In 2013, after a decade of partially successful reforms aimed at enhancing the country's cyber capabilities, the Chinese government became deeply concerned by the revelations in the leaks by US defector Edward Snowden. The leaks made evident the persistent difference between the US and China on cyber capacity, and notably the fragility of China's cyber defences [Swaine 2013]. The United States' employment of counter-technology is an example of the blurred borders between the government's objective of avoiding terrorist acts and public usage of defensive technologies [Balke 2018, *140–141*]. Chinese officials and academics also claim that most of the attacks on Chinese computers originate in the United States, with about 34.000 cyberattacks from the United States targeting China [Li and Xing 2012, *4*]. While the exact figures are debatable, it is undeniable that a large amount of malicious Internet activity originates from or passes through the United States.

Dependence on the US in terms of Internet configuration is another coercive factor [Raud 2016]. The Internet Corporation for Assigned Names and Numbers (ICANN) is located in California under federal US jurisdiction, even though it is technically independent of the US government [Raud 2016, *8*]. It is responsible for the management of Internet root name servers, domain name systems, and IP addresses worldwide, which creates dependability for all other states worldwide.

Before major reforms, China considered itself a vulnerable target overshadowed by American dominance in information technologies and military offense/defense capacities. A study produced by the National Computer Network Emergency Response Technical Team/Coordination Center of China named America, Canada and Russia as the top sources of hostile cyberattacks on Chinese targets at 63 percent, 17 percent and 2 percent respectively. The same research indicates 14.752 Trojan or botnet-infected

servers based in the U. S. controlled 3.34 million host computers within China in 2018, an increase of 90.8 percent from 2017 [Jiang 2020, *15*].

Based on the analysis of Swaine [2013], many quasi- and nonauthoritative Chinese sources assert that U. S. dominance and de facto control over Internet technologies and the cyberinfrastructure is unfair, presenting a source of instability and potential danger for the global cybersystem. Chinese government sources and academic circles raised similar concerns. After studying the trends in US-China rivalry in the field of ICT security during 2010–2015, Wang Xiang [2016] warns about the risk of falling into "Thucydides Trap" because of getting trapped in rivalry over cybersecurity issues, while the driving force behind the ongoing expansion of cyber capabilities in both countries is the lack of trust [Wang 2016, *39*; Levite and Lyu 2019]. The interests of US and China differ along five domains: ideological, security regulation, diplomacy, international trade and in the research field. Fudan University Professor Cai Cuihong [2018] also reviews US-China relations regarding Internet space regulation from geopolitical lens and indicates that the cyber game led by the United States poses a threat to the global cyber security situation.

The newly released 2019 white paper states the Chinese military needs to adapt to the "new era" of strategic competition by strengthening its preparedness and improving its combat capabilities to match China's global standing while preserving global peace [The State Council Information Office 2019]. The white paper makes it clear that China is interested in applying cutting-edge technologies to the military domain including artificial intelligence, big data, cloud computing, quantum computing, and the Internet of Things (IoT) [Jiang 2020].

The Washington's continual criticism of Chinese policies reinforces the Chinese government's isolationist stance. As a result, China has increased its Internet security and developed its own information technology in recent years as part of its quest for technical independence. For example, starting from 2015, 15 percent of computers in official offices across China have started to convert from Windows to Chinese-owned operating systems [Balke 2018, *147*]. Mikk Raud also writes that since China is concerned about the US using its status and influence as the world's leading technology power to establish international rules and norms, Beijing often justifies its actions in cyberspace as a response to hostile developments by the US military [Raud 2016, *7–8*].

China saw itself not as an initiator, but rather a victim of cyberattacks [Balke 2018], often condemning similar hacking by the United States of Chinese computer systems. The rapid changes brought about by the strengthening of US position in the cyberspace, led China to recognize the weaknesses in the domestic cybersecurity industry and come up with more drastic political, legal and military measures.

Mimetic. Originally, mimetic isomorphism refers to imitating successful organizations when an organization is uncertain about which strategy to pursue. When applied to the study of national cybersecurity frameworks, some states can follow the suit of a particular "model" state as a point of reference. In the case of China, more often than not, new trends in cybersecurity in Western states push Chinese officials to encourage local response, often mirroring the actions of others and adapting them to national needs.

EU's movement towards General Data Protection Regulation (GDPR) nudged China to establish more robust personal data protection policies [Jiang 2020] and it forged its own path towards personal data protection. Passed in 2017, China's Cybersecurity

Law like the GDPR outlines the rights of data objects, specifies the obligations for data controllers, and endorses the principles of data security, user consent, minimization of data collection, data anonymization and other protective measures. Similar to GDPR, China's Law guarantees a range of rights for data subjects. However, the rights provided in China's Cybersecurity Law are more limited in type and scope.

EU's GDPR was finally approved and entered into force in 2018 and its influence on China's legal relations continued. On 1 November 2021, the Chinese government introduced the Personal Information Protection Law (PIPL) that attempts to comprehensively regulate the storage, transfer, and processing of personal data [NPC 2021]. At first, it seemed that China would use the US's simpler regulatory structure as a blueprint for creating its own. However, there was a shift towards the European GDPR not long after.

The final text confirms these "mimetic" efforts, since large sections of the document contain similar regulations and even almost identical phrases. For example, similar to GDPR, the PILP also sets out the specific rights which data subjects are entitled to under it and sets up obligations for the personal information processor [Zhang, 2021]. Regarding personal individual information rights, the PIPL also aligns extensively with the GDPR [Deng and Dai 2021]. "Personal information" and "processing of personal information" are defined similarly in both the GDPR and the PIPL. Similarly to the GDPR, the PIPL extends its territorial scope to the processing of personal information outside of China and requires organizations to have a lawful basis to process personal information [Ke… 2021]. The newly enacted PIPL is more focused with safeguarding individual rights and interests against large digital businesses. It also serves two additional purposes for the Party and state leadership: first, it is a component of the broader anti-corruption campaign, which is expected to increase public trust in institutions; secondly, it fits into a strategy of regulating and restricting digital firms [Daum 2021].

Normative. In organizational theory, normative isomorphism refers to professional standards and practices established by education and training methods, professional networks, and movements of employees among firms [DiMaggio and Powell 1991, *68–73*]. In political science, it refers to compliance with international norms and community expectations [Singh and Alshammari 2020]. However, divergences in national laws and interpretation of present international standards are still being handled, and not every single element of how international law and its specialized bodies relate to cyber operations has been sorted out yet. Internet governance, Internet freedom, online privacy, cyber espionage, cyber-crime, and cyber wars are just a few of the topics that lie under the umbrella of cybersecurity rules [Clarke 2013, *11*].

Since accessing the Internet in 1994, China has formulated various forms of international network policies to integrate into the international cyberspace system. To integrate into globalization, one must fully participate in the international system. With China's growing influence in international affairs and increasing dependence on the Internet, active participation in cyberspace governance is also an important path and way to safeguard national interests. China's cyber policy is largely influenced by the international cyberspace governance situation, and has been developed and improved in the interaction with the international cyberspace governance system, showing the characteristics of multi-domain, multi-level and multi-subject [Lu 2016].

Clarke [2013] writes that in terms of cyber governance there are currently two opposing visions: US and many European states are in favour of multistakeholder

approach and advocate that non-profit organizations such as ICANN, ruled the Internet, while China and Russia are more inclined to support the central role of the ITU in the regulation of norms and standards [Clarke 2013, *13*; Ping 2018].

China is also one of the strongest proponents of cyber sovereignty. According to China's official position, cyber sovereignty serves as the cornerstone for a new international code of conduct for cyberspace, which extends the UN Charter's principle of sovereignty to cyberspace. Huang and Mačák [2017] oppose the idea of focusing too much on studying the division between these competing camps. Rather, the emerging picture reveals a web of relationships and views that reflect an overall trajectory of convergence, even if modest in scope. Ultimately, all states bear responsibility for collaboration and the dangers of isolation in the area of global cyber governance.

The building by the international community of an international cyber security architecture is still in the early stages of exploration, and cooperation and dialogue on cyber security issues are taking place simultaneously at several levels, including global (United Nations), regional (NATO, EU, Shanghai Cooperation Organization) and bilateral mechanisms. The UN and its member states reviewed two primary procedures in defining international cyber rules, one sponsored by the US and the other by Russia, during the UN's first global forum on cyber norms in September 2019. The Russia-backed Open-Ended Working Group (OEWG) focuses on achieving an agreement on internet sovereignty and non-interference in nations' political affairs, whereas the US-backed Group of Governmental Experts (GGE) stresses a free and open cyberspace environment [Kiyan 2021]. While there have been few state-led attempts to interpret existing or generate new legal standards, some nations have been able to agree on voluntary, politically binding confidence-building measures (CBMs). For example, in December 2013, the OSCE's member parties, including the United States and Russia, endorsed a list of 11 cyber-related CBMs.

Bilateral collaboration sometimes precedes multilateral accords, and cyber standards are frequently developed between the most sophisticated cyber nations. For example, in 2013, the United States and Russia reached an agreement on ICT-related CBMs, and in 2015, the United States and China negotiated an accord governing cyber operations. The Budapest Convention on Cybercrime, signed back in 2001, is currently the largest binding agreement on legal aspects of cybercrime. Even though it includes 65 states, neither China nor Russia are its members.

China's activities around international legal rules in cyberspace have been at an all-time high since 2014, when China began developing a digital military strategy. The dedication was also demonstrated by a governmental restructure that resulted in the establishment of the Chinese Cyberspace Administration, which was tasked with assisting the newly reorganized Central Leading Group on Informatization and Cyber Security. China's stance to international legal principles for cyberspace has also changed as a result of these actions [Austin 2016, *197*].

Taking into account the scarcity of binding intra-governmental agreements in cyber regulation, Chinese government is determined to use the momentum and become a norm-setter either by opposing the Western states in some of principles or by seeking common ground on bilateral level in areas which can benefit China's national interests. From the Chinese perspective, the existing multi-stakeholder platforms are fragmented and divided with limited function and authorization, and confined to specific areas, regions or interests, with the overall framework lacking in design and coordination.

Instead, China prefers the multilateral model, which is top-down, state-centric, and coordinated in nature. As it ascribes a decisive role to national governments, the primary forum for this governance model is the UN and its specialized agency, the ITU [Huang and Mačák 2017, *18*]. Same principles were outlined in the International Strategy of Cooperation on Cyberspace published by China's Ministry of Foreign Affairs and the Cyberspace Administration of China in 2017.

Instead of fragmenting Internet governance, China, according to Mueller [2017], practices alignment, motivating other nations to internalize and embrace a model of Internet governance that "re-aligns control of communications with national state jurisdictional borders" [Huang and Mačák, 2017, *18–19*]. This attitude is mirrored in China's five-year plan for 2016–2020, which for the first time officially recommends that China "actively engages in the establishment of international norms on the Internet". Chinese officials have regularly used the image of cyberspace as a road system with considerable traffic but no comprehensive "traffic laws" to justify their position. The combined Sino-Russian proposal for an International Code of Conduct for Information Security is the first such attempt to draft such "traffic regulations" with global reach, at least in Asia. Many of the themes of the SCO's formal 2009 Information Security Agreement are reflected in the Yekaterinburg Agreement. In addition, in 2015, China and Russia signed a bilateral agreement aiming at enhancing information security cooperation between the two nations.

These actions, taken together, demonstrate China's intention to extend its position in global governance, based on the belief that it should shift from being a "rule taker" to a "rule creator". To achieve this, Chinese government has tailored all of its domestic regulations and strategies to conform with the principle of "cyber sovereignty" and chose to keep pushing its agenda at the OEWG process. It signals of China's intention to focus on the UN as the primary norm-setting body and take an active role in the negotiations of the OEWG till 2025 as opposed to engaging into binding multi-party agreements outside the UN-framework.

Conclusion. Over the course of the past decade, China has built a solid cybersecurity framework and formulated the main policy goals in a set of strategic documents. The government's vision was backed by actual institutional reorganization within civil and military agencies based on the existing expertise of multiple departments responsible for network security. Just like many states around the globe were dormant about active reforms of the cybersecurity field at the beginning of the 21st century, the first initiatives by the Chinese government lacked strategic coherence, clear distinction of responsibilities among institutions, and incentives to take a proactive stance on the global arena regarding Internet governance.

Three types of pressures discussed in the article – coercive, mimetic, and normative – contributed to the study of various variables affecting the formation of China's national cybersecurity policy. Rising concerns about cyber military and espionage activities of the US (revealed after the NSA scandal in 2013), increasing effort in the US to develop its cyber military power spiked the debates about China's dependence on the US in the Internet field, and downsides of the national level of cybersecurity. By paying close attention to the legal and governmental reforms in the cyber field by Western states, the Chinese government reacted by introducing independent yet "mirroring" reforms and decided to become the main promoter of the "cyber sovereignty" doctrine in the further formation of the global Internet governance principles in opposition to the US-led coalition.

The formation of the future international order in cyberspace is mainly manifested in the play of values, the choice of institutional platforms and rule-making, while the evolutionary mechanism for the formation of order depends on the power play between countries and between state and non-state actors. The trend of cooperation and competition between China and the United States is likely to become be an important benchmark for establishing international order in cyberspace.

Finally, it can be observed that in China, the government is driving major cybersecurity policy reforms since 2014. Rapid institutional reorganization improved the decision-making and execution mechanisms both for civil and military structures. However, China still has a long way to go to align the actual readiness of private enterprises (both foreign and domestic) and the society with the policy goals. This is especially difficult given the size of the economy and the demographic factors. Pragmatic allocation of resources, heavy emphasis on security and control, as well as increased efforts to expand the number of well-qualified domestic experts in the field can significantly contribute to China's leadership in the field of cyber governance.

BIBLIOGRAPHY

蔡翠红 (2018). 网络地缘政治:中美关系分析的新视角. 国际政治研究, 1, pp. 9–37.

李侃如, 辛格彼得 (2012). 网络安全与美中关系. Brookings, available at: https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_Chinese.pdf.

鲁传颖 (2016). 网络空间治理的力量博弈、理念演变与中国战略. 国际展望, 8(01), pp. 117–134+157.

平郎 (2018). 网络空间国际秩序的形成机制. 国际政治科学, 3(1).

王翔 (2016). 中美网络安全领域博弈机理分析及未来展望. 中国与国际关系学刊, 2, pp. 34–51.

Austin G. (2016). "International Legal Norms in Cyberspace: Evolution of China's National Security Motivations" / In: A.-M. Osula and H. Rõigas (eds.), *International Cyber Norms Legal, Policy & Industry Perspectives*. Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, pp. 171–201.

Austin G. (2018). Cybersecurity in China: the next wave. Cham, Switzerland : Springer.

Balke L. (2018). "China's New Cybersecurity Law and U.S.-China Cybersecurity Issues". *Santa Clara Law Review*, 58(1).

Björck F. (2004). "Institutional theory: a new perspective for research into IS/IT security in organizations". *Proceedings of the 37th Hawaii International Conference on System Sciences*.

Clarke R. (2013). Securing Cyberspace Through International Norms. Good Harbor Security Risk Management.

Cyber Magazine (2021). China launches three-year cybersecurity action plan. *Cyber Security*. (online) *Cyber Magazine*, available at: https://cybermagazine.com/cyber-security/china-launches-three-year-cybersecurity-action-plan (Accessed 20 Jan. 2022).

Daddi T., Bleischwitz R., Todaro N. M., Gusmerotti N. M., & De Giacomo M. R. (2019). "The influence of institutional pressures on climate mitigation and adaptation strategies". *Journal of Cleaner Production*, *244*, 118879.

Daum T. (2021). A Chinese law made in Europe, available at: https://www.ips-journal.eu/work-and-digitalisation/a-chinese-law-made-in-europe-5596/#:~:text=China (Accessed 3 Feb. 2022).

Deng Z. and Dai J. (2021). The comparison between China's PIPL and EU's GDPR: Practitioners' perspective, available at: https://www.dentons.com/en/insights/articles/2021/october/8/the-comparison-between-chinas-pipl-and-eus-gdpr.

DiMaggio P. and Powell W. (eds.) (1991). *The New institutionalism in organizational analysis*. Chicago : The University of Chicago Press.

Ghosh P. (2021). China Now Has Almost 1 Billion Internet Users. (online) *Forbes,* available at: https://www.forbes.com/sites/palashghosh/2021/02/04/china-now-has-almost-1-billion-internet-users/?sh=2741d76526d9 (Accessed 22 Jan. 2022).

Hovav A., & D'Arcy J. (2012). "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U. S. and South Korea". *Information & Management*, 49(2), 99–110.

Huang Z. and Mačák K. (2017). "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches". *Chinese Journal of International Law*, 16(2), pp. 271–310.

ITU (2021). *Global Cybersecurity Index 2020*, available at: https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/ (Accessed 8 Nov. 2021).

Jepperson R. (1991). "Institutions, Institutional Effects, and Institutionalism". In: *The new institutionalism in organizational analysis*. Chicago : The University of Chicago Press, pp. 143–163.

Jeyaraj A. and Zadeh A. (2020). "Institutional Isomorphism in Organizational Cybersecurity: A Text Analytics Approach". *Journal of Organizational Computing and Electronic Commerce*, pp. 1–20.

Jiang M. (2020). "Cybersecurity policies in China" / In: L. Belli (ed.), *CyberBRICS: Cybersecurity Regulations in BRICS Countries*. Berlin, Germany : Springer, pp. 195–212.

Ke X., Liu V., Luo Y. and Yu Z. (2021). *Analyzing China's PIPL and how it compares to the EU's GDPR*, available at: https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/.

Kiyan O. (2021). Establishing Cybersecurity Norms in the United Nations: The Role of U. S.-Russia Divergence. *Harvard International Review*, available at: https://hir.harvard.edu/establishing-cybersecurity-norms-in-the-united-nations-the-role-of-u-s-russia-divergence/ (Accessed 4 Feb. 2022).

Levite A. and Lyu J. (2019). Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation? *Carnegie Endowment for International Peace,* available at: https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213.

Liang Saraf, Hu & Xue. (2007). "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management". *MIS Quarterly*, 31(1), 59.

Lindsay J. R., Tai Ming C. and Reveron D. S. (2015). China and cybersecurity: espionage, strategy, and politics in the digital domain. Oxford : Oxford University Press.

Mueller M. (2017). "Is cybersecurity eating internet governance? Causes and consequences of alternative framings". *Digital Policy, Regulation and Governance*, 19(6), pp. 415–428.

NPC (2021). 中华人民共和国个人信息保护法_中国人大网, available at: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

Osula A. N., Rõigas H. and NATO Cooperative Cyber Defence Centre Of Excellence (2016). *International cyber norms: legal, policy and industry perspectives*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre Of Excellence.

Peters G. (2019). Institutional Theory in Political Science: the new institutionalism. Edward Elgar Publishing.

Raud M. (2016). China and Cyber: Attitudes, Strategies, Organisation. Tallinn : NATO Cooperative Cyber Defence Centre of Excellence.

Safa N., Von Solms R. and Furnell S. (2016). "Information security policy compliance model in organizations". *Computers & Security*, 56, pp. 70–82, available at: https://www.sciencedirect.com/science/article/pii/S0167404815001583.

Scott R. (1995). Institutions and organizations: ideas, interests and identities. Sage Publications, Inc.

Singh H. P., & Alshammari T. S. (2020). "An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia". *Beijing Law Review*, 11(03), 637–650, available at: https://doi.org/10.4236/blr.2020.113039.

Swaine M. (2013). "Chinese Views on Cybersecurity in Foreign Relations". *China Leadership Monitor*, 42.

Teo H., Wei K., & Benbasat I. (2003). "Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective". *MIS Quarterly*, 27(1), 19, available at: https://doi.org/10.2307/30036518.

The International Institute for Strategic Studies (2021). "Cyber Capabilities and National Power: A Net Assessment". UK : The International Institute for Strategic Studies.

The State Council (2021). China's digital economy reaches $6t in 2020, available at: http://english.www.gov.cn/news/videos/202109/28/content_WS61527f60c6d0df57f98e0ff2.html#:~:text=China (Accessed 23 Jan. 2022).

The State Council Information Office (2019). China's National Defense in the New Era. available at: https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

Voo J., Hemani I., Jones S., DeSombre W., Cassidy D. and Schwarzenbach A. (2020). National Cyber Power Index 2020. Cambridge : Belfer Center for Science and International Affairs, Harvard Kennedy School.

Xinhua (2017). International Strategy of Cooperation on Cyberspace, available at: http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_2.htm.

Xu L. (2014). "China's Internet Development and Cybersecurity – Policies and Practices". In: *Chinese Cybersecurity and Defense*. London : ISTE Ltd, pp. 1–54.

Zheng D., Chen J., Huang L. and Zhang C. (2013). "E-government adoption in public administration organizations: integrating institutional theory perspective and resource-based view". *European Journal of Information Systems*, 22(2), pp. 221–234.

REFERENCES

Cài Cuìhóng (2018), "Kiberheopolityka: nova perspektyva dlya analizu kytays'ko-amerykans'kykh vidnosyn". *Guójì zhèngzhì yánjiū*, 1, pp. 9–37.

Lǐ Kǎnrú, Xīn Gé Bǐ Dé (2012), *Kiberbezpeka ta vidnosyny SSHA ta Kytayu.* Brookings, available at: https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_Chinese.pdf.

Lǔ Chuányǐng (2016), Sylova hra, evolyutsiya kontseptsiyi ta stratehiyi Kytaya v upravlinni kiberprostranstvom. *Guó jì zhǎn wàng* , 8(01), pp. 117–134+157.

Píng Láng (2018), Mekhanizm formuvannya mizhnarodnoho poryadku v kiberprostori. *Guójì zhèngzhì kēxué*, 3(1).

Wáng Xiáng (2016), Analiz ihrovoho mekhanizmu ta maybutnikh perspektyv u sferi kiberbezpeky mizh Kytayem ta SSHA. *Zhōngguó yǔ guójì guānxì xué kān*, 2, pp. 34–51.

Austin G. (2016), "International Legal Norms in Cyberspace: Evolution of China's National Security Motivations". In: A.-M. Osula and H. Rõigas, eds., *International Cyber Norms Legal, Policy & Industry Perspectives*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, pp. 171–201.

Austin G. (2018), *Cybersecurity in China: the next wave*. Cham, Switzerland: Springer.

Balke L. (2018), "China's New Cybersecurity Law and US-China Cybersecurity Issues". *Santa Clara Law Review*, 58(1).

Björck F. (2004), "Institutional theory: a new perspective for research into IS/IT security in organizations". *Proceedings of the 37th Hawaii International Conference on System Sciences*.

Clarke R. (2013), *Securing Cyberspace Through International Norms*. Good Harbor Security Risk Management.

Cyber Magazine (2021), *China launches three-year cybersecurity action plan | Cyber Security*. (online) Cyber Magazine, available at: https://cybermagazine.com/cyber-security/china-launches-three-year-cybersecurity-action-plan (Accessed 20 Jan. 2022).

Daddi T., Bleischwitz R., Todaro N. M., Gusmerotti N. M., & De Giacomo M. R. (2019), "The influence of institutional pressures on climate mitigation and adaptation strategies". *Journal of Cleaner Production*, *244*, 118879.

Daum T. (2021), A *Chinese law made in Europe*, available at: https://www.ips-journal.eu/work-and-digitalisation/a-chinese-law-made-in-europe-5596/#:~:text=China (Accessed 3 Feb. 2022).

Deng Z. and Dai J. (2021), *The comparison between China's PIPL and EU's GDPR: Practitioners' perspective*, available at: https://www.dentons.com/en/insights/articles/2021/october/8/the-comparison-between-chinas-pipl-and-eus-gdpr.

DiMaggio P. and Powell W. eds., (1991), *The New institutionalism in organizational analysis*. Chicago: The University of Chicago Press.

Ghosh P. (2021). *China Now Has Almost 1 Billion Internet Users*. (online) Forbes, available at: https://www.forbes.com/sites/palashghosh/2021/02/04/china-now-has-almost-1-billion-internet-users/?sh=2741d76526d9 (Accessed 22 Jan. 2022).

Hovav A., & D'Arcy J. (2012), "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U. S. and South Korea". *Information & Management*, 49(2), 99–110.

Huang Z. and Mačák K. (2017), "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches". *Chinese Journal of International Law*, 16(2), pp. 271–310.

ITU (2021), *Global Cybersecurity Index 2020*, available at: https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/ (Accessed 8 Nov. 2021).

Jepperson R. (1991), "Institutions, Institutional Effects, and Institutionalism". In: *The new institutionalism in organizational analysis*. Chicago: The University of Chicago Press, pp. 143–163.

Jeyaraj A. and Zadeh A. (2020), "Institutional Isomorphism in Organizational Cybersecurity: A Text Analytics Approach". *Journal of Organizational Computing and Electronic Commerce*, pp. 1–20.

Jiang M. (2020), "Cybersecurity policies in China". In: L. Belli (ed.), *CyberBRICS: Cybersecurity Regulations in BRICS Countries*. Berlin, Germany: Springer, pp. 195–212.

Ke X., Liu V., Luo Y. and Yu Z. (2021), *Analyzing China's PIPL and how it compares to the EU's GDPR*, available at: https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/.

Kiyan O. (2021), *Establishing Cybersecurity Norms in the United Nations: The Role of US-Russia Divergence*. Harvard International Review, available at: https://hir.harvard.edu/establishing-cybersecurity-norms-in-the-united-nations-the-role-of-u-s-russia-divergence/ (Accessed 4 Feb. 2022).

Levite A. and Lyu J. (2019), *Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?* Carnegie Endowment for International Peace, available at: https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213.

Liang Saraf, Hu & Xue. (2007), "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management". *MIS Quarterly*, 31(1), 59.

Lindsay J. R., Tai Ming C. and Reveron D. S. (2015), *China and cybersecurity: espionage, strategy, and politics in the digital domain*. Oxford: Oxford University Press.

Mueller M. (2017), "Is cybersecurity eating internet governance? Causes and consequences of alternative framings". *Digital Policy, Regulation and Governance*, 19(6), pp. 415–428.

NPC (2021), *Zakon Kytays'koyi Narodnoyi Respubliky pro zakhyst personal'noyi informatsiyi*, available at: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

Osula A. N., Rõigas H. and NATO Cooperative Cyber Defence Centre Of Excellence (2016), *International cyber norms: legal, policy and industry perspectives*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre Of Excellence.

Peters G. (2019), *Institutional Theory in Political Science: the new institutionalism.* Edward Elgar Publishing.

Raud M. (2016), *China and Cyber: Attitudes, Strategies, Organization*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Safa N., Von Solms R. and Furnell S. (2016), "Information security policy compliance model in organizations". *Computers & Security*, 56, pp. 70–82, available at: https://www.sciencedirect.com/science/article/pii/S0167404815001583.

Scott R. (1995), *Institutions and organizations: ideas, interests and identities*. Sage Publications, Inc.

Singh H. P., & Alshammari T. S. (2020), "An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia". *Beijing Law Review*, 11(03), 637–650, available at: https://doi.org/10.4236/blr.2020.113039.

Swaine M. (2013), "Chinese Views on Cybersecurity in Foreign Relations". *China Leadership Monitor*, 42.

Teo H., Wei K., & Benbasat I. (2003), "Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective". *MIS Quarterly*, 27(1), 19, available at: https://doi.org/10.2307/30036518.

The International Institute for Strategic Studies (2021), "Cyber Capabilities and National Power: A Net Assessment". UK: The International Institute for Strategic Studies.

The State Council (2021), *China's digital economy reaches $6t in 2020*, available at: http://english.www.gov.cn/news/videos/202109/28/content_WS61527f60c6d0df57f98e0ff2.html#:~:text=China (Accessed 23 Jan. 2022).

The State Council Information Office (2019), *China's National Defense in the New Era*, available at: https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

Voo J., Hemani I., Jones S., DeSombre W., Cassidy D. and Schwarzenbach A. (2020), *National Cyber Power Index 2020*. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Xinhua (2017), *International Strategy of Cooperation on Cyberspace*, available at: http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_2.htm.

Xu L. (2014), "China's Internet Development and Cybersecurity – Policies and Practices". In: *Chinese Cybersecurity and Defense*. London: ISTE Ltd, pp. 1–54.

Zheng D., Chen J., Huang L. and Zhang C. (2013), "E-government adoption in public administration organizations: integrating institutional theory perspective and resource-based view". *European Journal of Information Systems*, 22(2), pp. 221–234.

Стаття надійшла до редакції 02.02.2022