Історико-політичні проблеми сучасного світу: Збірник наукових статей. – Чернівці: Чернівецький національний університет, 2022. – Т. 45. – С. 113-127
DOI: 10.31861/mhpi2022.45.113-127

Modern Historical and Political Issues: Journal in Historical & Political Sciences. – Chernivtsi: Chernivtsi National University, 2022. – Volume. 45. – pp. 113-127
DOI: 10.31861/mhpi2022.45.113-127

УДК 327(73+510):[351.746:007

© Сергій Федонюк [1]
© Сергій Магдисюк [2]

Протистояння між США й Китаєм у сфері кібербезпеки

Досліджено глобальну конкуренцію США і Китаю в сфері кібербезпеки. Встановлено характер і тенденції протистояння між країнами в сфері кібербезпеки, досліджено цілі, засоби кібернетичних впливів у протистоянні США й Китаю в цій сфері, встановлено напрями їх розвитку.

Проаналізовано характер і напрями розвитку негативних кібернетичних впливів з точки зору кожної зі сторін. Розглянуто основні приклади кібернетичних впливів і позиції США й Китаю щодо взаємних кібернетичних загроз. Установлено стратегічні цілі кібер-впливів у різні періоди та їх зв'язок із стратегічними пріоритетами країн в аспекті їх міжнародної діяльності, зокрема з позиції китайської стратегії «багатополярного» світу й діяльності адміністрації президента США, спрямованої на консолідацію країн Заходу перед кіберзагрозами з боку Китаю. Визначено особливості актуальних тенденцій у протистоянні між США й Китаєм у сфері кібербезпеки з урахуванням стратегічних цілей обох держав.

Ключові слова: США, Китай, кібербезпека, протистояння

US-China Confrontation in Cyber Security

This study presents the research results of the activities of the United States and China as the major global competitors in the field of cybersecurity. We have established the nature and trends of the confrontation, explored the goals and means of cyber influences in the confrontation between two states in this area, and identified directions for the development of the competition between the United States and China in the field of cybersecurity.

Today, the United States and China are the world leaders in cyberspace and the information (cyber) security sector. The United States remains the undisputed world leader in cybersecurity, but China is rapidly closing the gap, relying on the strong potential of human and economic resources in cyberspace. From the beginning of the second decade of the XXI century. countries have been accusing each other of cyberattacks for economic purposes and cyber espionage. The United States has pointed to the People's Liberation Army's (PLA) leading role in organizing cyberattacks, and China has made similar allegations against the US intelligence. Despite attempts to reconcile policies in this area, tensions between the United States and China over cyber-building are growing. And since the beginning of the 2020s, politically motivated influences on information systems have become the target of cyberattacks. The United States notes a change in China's cyberattack strategy from regular cyber espionage to prosecuting political and security goals. Additionally, systematic control over the sources of cyber threats has been transferred from the PLA to the security structures of China.

China also accuses the United States of using cyber influences to increase world hegemony and using cyber threats in the arms race. Beijing makes these statements from the standpoint of its own "multipolar" world strategy, which is threatened by the activities of the Joe Biden administration, aimed at consolidating Western countries in the face of cyber threats from China.

The field of cybersecurity in US-China relations is becoming increasingly important in terms of the security strategies of these two world leaders. Each of them uses cyber tools as a tool of cyber influ-

[1] Кандидат географічних наук, доцент кафедри міжнародних комунікацій та політичного аналізу, Волинський національний університет імені Лесі Українки, Україна. E-mail: sergii.fedoniuk@vnu.edu.ua; https://orcid.org/0000-0003-2853-8905.

[2] Магістр, Волинський національний університет імені Лесі Українки, Україна. E-mail: mahdysiuk.serhii @vnu.edu.ua.

ence, as well as a tool for strategic communication at the level of relations with strategic partners. Therefore, these issues will become increasingly important in terms of research interests, in particular the implementation of foreign policy interests in relations with these countries.

Keywords: USA, China, cybersecurity, confrontation.

Постановка наукової проблеми та її значення. Сьогодні фіксується різке збільшення масштабів активності зловмисних груп, що фінансуються державами й організованою злочинністю[3]. Безпосередніми наслідками кіберзлочинності є пошкодження та знищення даних, крадіжка інтелектуальної власності й персональних та фінансових даних, шахрайство, загроза бізнес-комунікаціям і діловій репутації та ін. Окремі атаки можуть загрожувати критичній інфраструктурі, впливати на перебіг виборчих кампаній, дестабілізувати економічну й політичну ситуацію. Вважається, що США й Китай сьогодні є головними міжнародними акторами й бенефіціарами безпекової сфери кіберпростору[4]. Ці країни залишаються найбільшими конкурентами на світовій арені й глобальному ринку інформаційних і комунікаційних технологій. Водночас загострюються й безпекові суперечності між цими найбільшими військово-політичними потугами. Оскільки у зв'язку зі зростанням значення ІКТ ця конкуренція все більше охоплює й кіберпростір, науковий інтерес становить проблема виявлення і аналіз актуальних взаємних викликів у сфері кіберзагроз і тенденцій в кібербезпеці цих країн.

Аналіз останніх досліджень із цієї проблеми. Діяльність США й Китаю у сфері кібербезпеки досліджується низкою авторів, які зосереджені на різних аспектах. Зокрема – це концептуальні й правові питання політики Китаю в сфері кабербезпеки (Чанг[5], Сіньмінь[6], Вень Лі[7]); окремі питання в аспекті кіберзагроз у відносинах між США й Китаєм (Чон[8], Остін[9], Карр[10], Лін Фей[11], Гарольд, Лібіцкі і Цевальос[12]); особливості міжнародної політики Китаю в цій сфері (Свейн[13]). У контексті міжнародної взаємодії США й Китаю досліджено різноманітні проблеми кібербезпеки, актуальні з точки зору двосторонніх відносин і глобального розвитку (наприклад Лібертал[14], Даймонд і Карсон[15], Паркер[16]) При цьому залишається широке поле

[3] Morgan, S. (2021). 2021 Report: Cyberwarfare in the C-suite, Cybersecurity Ventures, available at: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf (accessed March 10, 2022).

[4] Deibert, R. (2015). Trajectories for Future Cybersecurity Research. *The Oxford Handbook of International Security*. Ed. by A. Gheciu and W. C. Wohlforth. Oxford: Oxford University Perss, p. 531-556; Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. *International Security,* Vol. 39. №. 3, p. 7-47.

[5] Chang, A. (2015). *Warring State: China's Cybersecurity Strategy.* Washington, D.C.: Center for a New American Security, December 2015, p. 7 and 10.

[6] Xinming, M. (2015). What Kind of Internet Order Do We Need? *Chinese Journal of International Law,* Vol. 14. No. 2, 2015, p. 399–403.

[7] Wenli, Yi. (2012). Divergence Between China and the U.S. and the Path Toward Cooperation in Cyberspace ["Zhong-Mei zai Wangluo Kongjian de Fenqi yu Hezuo Lujing"], *Contemporary International Relations* [Xiandai Guoji Guanxi], Vol. 22, No. 4, July/August 2012, p. 124–141.

[8] Chong, J. (2010). Cyber: The Invisible New Battlefront [Wangluo: Kanbujian de xin zhanxian], *Seeking Truth* [Qiu Shi], No. 13, 2010, p. 53–55.

[9] Austin, G. (2015). No Easy Solutions in U.S.-China Cyber Security. *East Asia Forum,* October 6, 2015.

[10] Carr, J. (2015). Cyber Attacks: Why Retaliating Against China Is the Wrong Reaction. *The Diplomat,* August 6, 2015.

[11] Linfei, Zh. (2015). Commentary: U.S. Should Think Twice Before Retaliating Against China over Unfounded Hacking Charges. *Xinhua,* August 3, 2015.

[12] Harold, S. W., Libicki, M. C., & Cevallos, A. S. (2016). The "Cyber Problem" in U.S.-China Relations. In Getting to Yes with China in Cyberspace (pp. 1–16). RAND Corporation, available at: http://www.jstor.org/stable/10.7249/j.ctt1cx3vfr.6 (accessed March 10, 2022).

[13] Swaine, M. D. (2013). Chinese Views of Cybersecurity in Foreign Relations. *China Leadership Monitor,* No. 42, fall 2013.

[14] Lieberthal, K. (2012). Cybersecurity and U.S. – China Relations. Jonh L. Torton China Institute in Brookings. 52 p., available at: https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf (accessed March 10, 2022).

для досліджень у зв'язку з новими подіями й розвитком політики головних міжнародних акторів в цій сфері.

Формулювання мети та завдань статті. Метою дослідження є встановлення характеру й тенденцій протистояння між США й Китаєм у сфері кібербезпеки. До завдань належать дослідження цілей і засобів кібернетичних впливів у протистоянні США й Китаю та встановлення напрямів їх розвитку.

Виклад основного матеріалу

Кібербезпека як сфера конкуренції між США й Китаєм

США і КНР – дві найбільші економіки світу – є глобальними лідерами в сфері кібербезпеки. При цьому, Сполучені Штати безумовно залишаються найбільш кіберспроможною країною у світі. Такий висновок міститься у доповіді Cyber Capabilities and National Power 2021, опублікованій в червні 2021 р. британським аналітичним центром Міжнародного інституту стратегічних досліджень, у якій розглядаються кібер-здатності 15-ти найбільших світових гравців у сфері хакерства та цифрового захисту. У звіті оцінюються можливості як уряду, так і приватного сектора. Документ відносить найбільш потужних супротивників США, Росію та Китай до другого рівня кіберпотужності, так само, як Великобританію, Канаду, Австралію, Ізраїль і Францію[17].

Китай досяг значного прогресу в зміцненні своїх кібер-можливостей, але далеко не настільки, щоб скоротити розрив із США. Головною причиною є відмінності у рівнях цифрових економік двох країн, де США залишаються далеко попереду, незважаючи на цифровий прогрес Китаю.

Така домінуюча позиція Сполучених Штатів пояснюється багатьма факторами, зокрема[18]:

– домінуючим військовим потенціалом як у наступальних, так і в оборонних кіберспроможностях;

– світового рівня персоналом американських технологічних компаній та компаній з кібербезпеки;

– системним державним підходом до кібербезпеки й управління ризиками.

Проте швидкий цифровий розвиток Китаю та зростаюча кількість технологічних фірм роблять його «єдиною державою, яка зараз має намір приєднатися до США на першому рівні кіберпотужності»[19].

Найважливішим фактором для підтримання загальної кіберспроможності країни є наявність кадрів вітчизняних компаній, зосереджених у сфері інформаційно-комунікаційних технологій, які можуть розвивати кібер-спроможності. Саме це дає Китаю з його чисельними технологічними й телекомунікаційними компаніями, що швидко розвиваються, найкращі шанси кинути виклик позиції Сполучених Штатів на вищому рівні.

Тема кібербезпеки – одна з найновіших у двосторонніх відносинах між Сполученими Штатами й Китаєм, чому сприяли швидкий розвиток технологій і зростаюча залежність суспільства від інтернету. Відтоді як суспільно-економічні відносини почали розвиватися в напрямі кіберпростору, а інтернет став основним середовищем інформаційної роботи й комунікації, стосунки між Сполученими Штатами й Китаєм ставали все більш напруженими. Це стало результатом

[15] Diamond, L., Carson, B. (2019). Jaw-Jaw: How Chinese Sharp Power Takes Aim at American Democracy. War on the Rocks. [online], February 5, 2019, available at: https://warontherocks.com/2019/02/jaw-jaw-how-chinese-sharp-power-takes- aim-at-american-democracy (accessed March 10, 2022).

[16] Parker, C. B. (2018). China Exerting „Sharp Power" Influence On American Institutions. *HOOVER*, Dec. 19, 2018 available at: https://www.hoover.org/news/china-exerting-sharp-power-influence-american-institutions (accessed March 10, 2022).

[17] IISS (2021). Cyber Capabilities and National Power: A Net Assessment. IISS. Research Papers, June 28, 2021, available at: https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/ (accessed March 10, 2022).

[18] Schaffer, A. (2021). The Cybersecurity 202: The United States is still number one in cyber capabilities. *The Washington Post*, June 28, 2021, available at: https://www.washingtonpost.com/politics/2021/06/28/ cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/ (accessed March 10, 2022).

[19] IISS (2021). Cyber Capabilities and National Power: A Net Assessment. IISS. Research Papers, June 28, 2021, available at: https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/ (accessed March 10, 2022).

посилення кіберзагроз і призвело до зростання взаємних звинувачень в кібершпигунстві[20]. США звинувачують КНР в тому, що з його боку часто здійснюються кібератаки з метою втручання в бізнес-інтереси та різні комерційні справи, що супроводжуються викраденням інформації, що становить комерційну таємницю, порушенням інтелектуальної власності у сфері нових технологій та іншої інформації з метою комерційної вигоди. І навпаки, Китай часто звинувачує Сполучені Штати в тому, що вони домінують в інтернеті й використовують своє панівне становище в кіберпросторі для збору розвідданих[21].

На підставі проведених розслідувань США мають підстави звинувачувати Китай у низці кібератак, реалізованих протягом тривалого періоду. Компанія Mandiant, що базується в Сполучених Штатах, виявила кілька так званих розширених постійних загроз (APT), які були здійснені з боку Китаю, часто із залученням інших країн, таких як Російська Федерація. У звіті компанії зазначається, що станом на 2013 р. існувало достатньо доказів, які показують обізнаність Китаю щодо заходів, які здійснюють різні групи кібершпигунства. Зокрема, діяльність, пов'язану із кібершпигунством, проводили члени підрозділу 61398 Народно-визвольної армії Китаю. У зазначеному звіті показано, що з 2006 р. до 2013 р. в ході такої активності (APT1) зламано й вкрадено сотні терабайтів інформації з понад 141 компанії, із яких 87 % базувалися в англомовних країнах. Найбільшою метою атак були Сполучені Штати, в яких базуються 115 зламаних компаній[22]. Можна припустити, що значна частина цілей хакерських атак в США пов'язана не лише з APT1, але й з багатьма іншими загрозами, які використовував китайський уряд.

У 2014 р. Міністерство юстиції США висунуло звинувачення п'ятьом чиновникам китайської армії в незаконному отриманні та розповсюдженні комерційної таємниці зі Сполучених Штатів на користь представників економічної сфери Китаю. Це був один із перших сигналів для КНР про те, що Сполучені Штати мають усе більше підстав звинувачувати Китай у причетності до кіберзлочинів. Після арешту та висунення звинувачення військовослужбовцям китайської армії в Сполучених Штатах, китайські ЗМІ назвали це помстою, щоб зберегти обличчя в ситуації з витоком інформації через колишнього співробітника американських спецслужб Едварда Сноудена. Пізніше того ж року Агентство національної безпеки США повідомило, що Китай здійснив величезну кількість кібератак проти Сполучених Штатів за короткий проміжок часу, і сотні з них були успішними[23].

З метою врегулювання протистояння між обома державами та координації боротьби із кіберзлочинністю тодішній президент Барак Обама запросив китайського лідера Сі Цзіньпіна відвідати США з державним візитом. Сполучені Штати хотіли забезпечити захист своїх корпорацій від крадіжки інтелектуальної власності. Зрештою, обидві сторони дійшли угоди, яку підписали в 2015 р., щодо посилення комунікації та співпраці між ними. Також у документі підтверджено, що жодна зі сторін не буде свідомо здійснювати крадіжку інтелектуальної власності в іншої, погоджено розробити й запропонувати належні норми поведінки між державами для кіберпростору в міжнародному співтоваристві[24].

Але зазначена вище угода проіснувала недовго, оскільки обидві сторони вчинили дії, що варіюються від загрозливих до незаконних. Протягом двох років після підписання Угоди про кібербезпеку між США та Китаєм у 2015 р. проблема крадіжки інтелектуальної власності не зменшилась, а набула іншої форми. Хакерські групи із КНР, замість того, щоб зосередитися на

[20] Julian N. (2021). United States' and China's Cybersecurity Policies: Collaboration or Confrontation? *Journal of International Relations*, January 24, 2021, available at:http://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation (accessed March 10, 2022).

[21] Brown, G., Yung, C. D. (2017a). Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace. *The Diplomat*, January 19, 2017, available at: https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/ (accessed March 10, 2022).

[22] Fireyes (2013). *Cyber Threat Intelligence on Advanced Attack Groups and Technology Vulnerabilities.* Threat Intelligence Reports. Fireyes, 2013.

[23] Brown, G., Yung, C. D. (2017b). Evaluating the US-China Cybersecurity Agreement, Part 3: Over a year later, what impact has the 2015 cyber agreement had on U.S.-China relations? *The Diplomat*, January 21, 2017, available at: https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/ (accessed March 10, 2022).

[24] Brown, G., Yung, C. D. (2017b). Там само.

крадіжці інтелектуальної власності компаній у Сполучених Штатах, як це було раніше, почали реалізувати різні форми шпигунства проти державних структур. Оскільки договір 2015 р. визначив умови, які забороняють крадіжку інтелектуальної власності, за технічними особливостями державні дані виходять за межі положень угоди. Хакери в Китаї також використовували злам, щоб проникнути в американські компанії, такі як Google й Intel[25].

Китайські атаки на фірми зі Сполучених Штатів і урядові ресурси не залишилися непоміченими. Адміністрація Дональда Трампа вдалася до заборони використання технологій китайських державних компаній, зокрема Huawei. Піком протистояння з компанією стало затримання її фінансового директора в Канаді. Навіть більше, як про це заявляють китайські дослідники, наприклад З. Су, «Сполучені Штати почали власну форму пропагандистської війни щодо Huawei у своїх спробах демонізувати корпорацію перед своїми союзниками, зокрема партнерами у рамках кіберугоди Five Eyes»[26]. Хоча не виключена ймовірність того, що оскільки Huawei і Китай зараз є світовими лідерами технології 5G, Сполучені Штати роблять спроби зупинити їх зростання. Зі свого боку, Китай звинувачує США в низці кібератак і кібершпигунських інцидентів.

Китай як джерело кіберзагроз для США

Історія питання. Китай активно розвиває свій кіберпростір, із чим пов'язана й активізація кіберзлочинності й виникнення інших кіберзагроз. Із початком епохи соціальних мереж і масового використання інтернету з метою ведення бізнесу стали з'являтися повідомлення про китайських кібер-злочинців і кібер-шпигунів. Але якщо десятиліття тому більшість виявлених фактів асоціювалася з використанням низькорівневих фішингових електронних листів проти американських компаній та крадіжкою інтелектуальної власності, то до сьогодні хакерські атаки з Китаю перетворилися на серйозно організовані операції, а сам Китай сприймається в США як досвідчений і зрілий супротивник[27].

У Сполучених Штатах Китай почали асоціювати з масштабним джерелом кіберзагроз після серії атак на початку другого десятиліття XX ст. У січні 2010 р. компанія Google заявила, що вона та більше 20 інших компаній стали жертвами складної кібератаки з боку хакерів із Китаю, що пізніше отримала назву Operation Aurora, яка призвела до крадіжки інтелектуальної власності. Хоча хакери ніколи не були публічно ідентифіковані, інцидент посилив напруженість між Вашингтоном і Пекіном через наявність непрямих доказів того, що значна кількість кібератак на американські інституції походить із Китаю. Представники IT-компанії Symantec повідомили, що хакери, які стоять за операцією «Аврора», зосередилися на крадіжці інтелектуальної власності, зокрема, проєктної документації в оборонних підрядників та їхніх постачальників, включаючи судноплавні, авіаційні, збройні, енергетичні, виробничі, інженерні й електронні компанії. Другою за поширеністю групою цілей хакерів були неурядові організації, що займаються питаннями прав людини в Тибеті, а третьою – фінансові фірми й компанії по виробництву програмного забезпечення[28].

У 2013 р. китайців звинувачено в атаці на видання New York Times. Хакери здійснювали маршрутизацію через мережу газети протягом щонайменше чотирьох місяців, викрадаючи паролі репортерів у очевидній спробі ідентифікувати джерела й зібрати інші розвідувальні дані про історії, пов'язані з сім'єю прем'єр-міністра Китаю Вен Цзябао. Злам збігся із розслідуванням, опублікованим газетою Times роком раніше, яке розглядало статки, що накопичила сім'я китайського прем'єра. Хакери зламали мережу, коли газета завершувала опрацювання ма-

[25] Greenberg, A. (2017). China tests the limits of its U.S. hacking truce. *Wired*, October 13, 2017, available at: https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/# (accessed March 10, 2022).

[26] Soo, Z. (2019). How Huawei beat America's anti-China 5G propaganda war in Southeast Asia, years before it even began. *South China Morning Post*, April 22, 2019, available at: https://www.scmp.com/tech/article/3006935/how-huawei-beat-americas-anti-china-5g-propaganda-war-southeast-asia-years-it (accessed March 10, 2022).

[27] Perlroth, N. (2021). How China Transformed Into a Prime Cyber Threat to the U.S. *The New York Times*, July 19, 2021, available at: https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html (accessed March 10, 2022).

[28] Finkle, J. (2012). Hundreds more cyber attacks linked to 2009 Google breach. *Reuters*, Sept. 12, 2012, available at: https://www.reuters.com/article/cybersecurity-espionage-idUSL2E8K7A9E20120907 (accessed March 10, 2022).

теріалів розслідування. Були зламані електронні пошти голови шанхайського бюро газети Девіда Барбози, який проводив розслідування, а також керівника південноазійського бюро газети в Індії Джима Ярдлі, який раніше працював у Пекіні[29].

У 2014 р. Президент США Барак Обама назвав кібератаки "реальною загрозою" безпеці й економіці США. Сполучені Штати звинуватили офіцерів китайської армії в кібер-зламі американських приватних компаній у спробі отримати конкурентну перевагу. Генеральна прокуратура США стверджує, що офіцери викрали комерційні таємниці й внутрішні документи у п'яти компаній і профспілки. Проте Китай відкинув звинувачення й попередив, що ця справа зашкодить американо-китайським відносинам[30].

Сполучені Штати, очевидно, мали підстави для таких звинувачень, оскільки на початку 2013 р. компанією Mandiant, що надає послуги в сфері кібербезпеки, опубліковано результати розслідування, у якому стверджується, що за сотні (а за деякими оцінками, тисячі) атак на американські компанії відповідав один шанхайський підрозділ Народно-визвольної армії Китаю (НВАК), відомий як підрозділ 61398. Mandiant відстежила окремих членів найактивніших китайських хакерських груп (таких як «Comment Crew» або «Шанхайська група») до «порога штабу військової частини»[31].

Підрозділ 61398 (формально 3-й відділ Управління Генерального штабу 2-го Бюро Народно-визвольної армії Китаю) майже ніде не згадується в офіційних китайських військових джерелах. Проте аналітики розвідки стверджують, що він є центральним елементом китайського комп'ютерного шпигунства, зосередженим на політичній, економічній і військовій розвідці[32]. У період 2002-2012 рр., за висновками американської компанії з кібербезпеки "Fireye", у рамках діяльності цієї групи здійснено понад тисячу кібератак проти великих компаній і відомих політиків. Невдовзі після першого візиту китайського лідера Сі Цзіньпіна до США в 2015 р. укладено угоду про те, що Китай припинить хакерські атаки на американські компанії для своєї промислової вигоди. Відтоді протягом 18-ти місяців, за часів адміністрації Обами, спостерігалося помітне зменшення інтенсивності китайського хакерства[33].

Після того, як президент Дональд Трамп вступив на посаду й ініціював торговельні конфлікти й інші напруження з Китаєм, хакерські атаки відновилися. Причому змінилися як їх джерело, так і суть. Хакери НВАК були відсторонені, і їх замінили оперативники, що працюють за дорученням Міністерства державної безпеки, яке керує розвідкою, безпекою й таємною поліцією Китаю. Тепер реалізатори кібер-нападів діють не з НВАК, а з «незалежної» мережі підставних компаній і підрядників, включаючи інженерів, які працювали на деякі з провідних технологічних компаній. Достеменно невідомо як саме Китай працював із цими слабо афілійованими хакерами – або їм платили готівкою, або в них не було іншого вибору, окрім як робити все, що просить держава[34].

Сучасний стан. Адміністрація Джозефа Байдена підняла боротьбу з кіберзагрозами на якісно новий рівень, перетворивши кібератаки, включаючи атаки програм-вимагачів, у великий дипломатичний фронт із конкуруючими державами, передусім Китаєм. Загострення уваги американського уряду до кіберзагроз пов'язано з тим, що кібер-зловмисники суттєво активізувалися в останні роки. Так, у липні 2021 р. Сполучені Штати звинуватили Китай у кібератаках,

[29] Zetter, K. (2013). New York Times Hacked Again, This Time Allegedly by Chinese. *Wired*, January 31, 2013, available at: https://www.wired.com/2013/01/new-york-times-hacked/ (accessed March 10, 2022).
[30] BBC (2014). US justice department charges Chinese with hacking. *BBC*, May 14, 2014, available at: https://www.bbc.com/news/world-us-canada-27475324 (accessed March 10, 2022).
[31] Atlantic Council (2013). Chinese Army unit is seen as tied to hacking against U.S. *Atlantic Council*, February 19, 2013. available at: https://www.atlanticcouncil.org/blogs/natosource/chinese-army-unit-is-seen-as-tied-to-hacking-against-us/ (accessed March 10, 2022).
[32] Fireyes (2013). Cyber Threat Intelligence on Advanced Attack Groups and Technology Vulnerabilities. Threat Intelligence Reports. *Fireyes*, 2013.
[33] The New York Times (2015). Obama and Xi Jinping of China Agree to Steps on Cybertheft. *The New York Times*, Sept. 25, 2015, available at: https://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html (accessed March 10, 2022).
[34] Wolfe, D. (2021). How China Became a Digital Adversary and Threat to the U.S. GSIExchange, July 21, 2021, available at: https://gsiexchange.com/how-china-became-a-digital-adversary-and-threat-to-the-u-s/ (accessed March 10, 2022).

відмітивши, що ці атаки були дуже агресивними, вони показують, що Китай перетворився на набагато більш витонченого й зрілого цифрового супротивника, ніж той, який хвилював американських чиновників десять років тому. Сполучені Штати та їхні союзники звинуватили Китай у глобальній кампанії кібершпигунства. Відтак зібрано надзвичайно широку коаліцію країн, до якої приєдналися члени НАТО, Європейського Союзу, Австралія, Великобританія, Японія й Нова Зеландія. За словами держсекретаря США Ентоні Блінкена із цього приводу, проблема кібератах становить «велику загрозу нашій економічній та національній безпеці» [35].

Одночасно міністерство юстиції США висунуло звинувачення чотирьом громадянам Китаю: трьом співробітникам служби безпеки і одному хакеру-зломщику – у нападі на десятки компаній, університетів і державних установ у Сполучених Штатах і за кордоном[36]. Відповідно до цієї заяви, громадяни Китаю діяли з підставних компаній, таких як Хайнань Сяньдунь, створених Міністерством державної безпеки, щоб дати китайським спецслужбам правдоподібне прикриття. Також були звинувачені китайські університети в тому, що вони відіграють важливу роль, набираючи студентів у підсобні компанії й керуючи їхніми ключовими бізнес-операціями, такими як нарахування заробітної плати. Обвинувальний акт також вказував на китайських «пов'язаних з урядом» хакерів, які проводили атаки програм, що вимагають у компаній мільйони доларів. Це свідчить про суттєві зміни в географії кіберзагроз такого типу, оскільки раніше атаки зловмисників-вимагачів основному походили з Росії, Східної Європи й Північної Кореї.

Звинувачення з боку адміністрації Президента США в кібератаках показують, що Китай за останні роки реорганізував свої хакерські операції. У той час, як колись він здійснював відносно прості хакерські атаки на іноземні компанії, аналітичні центри й державні установи, зараз КНР здійснює приховані, децентралізовані цифрові напади на американські компанії й інтереси в усьому світі.

За словами американських чиновників і представників ділових кіл, хакерські дії, які здійснювалися підрозділами НВАК через непрофесійно сформульовані електронні листи (фішинг), тепер здійснюються елітною мережею з підрядних компаній та університетів, які працюють за вказівкою Міністерства державної безпеки Китаю[37]. Хоча фішингові атаки залишаються актуальними, шпигунські кампанії пішли в підпілля й використовуються складні методи. Серед них – використання «нульових днів» або невідомих раніше «дір» у безпеці в поширеному програмному забезпеченні, як-от служба електронної пошти Microsoft Exchange і пристрої безпеки Pulse VPN. Від таких атак важче захиститися й вони дають змогу китайським хакерам працювати непоміченими протягом більш тривалого періоду[38]. У зв'язку з цим Д. Вольфе наводить цитату Джорджа Курца, виконавчого директора компанії з кібербезпеки CrowdStrike: «Те, що ми спостерігали протягом останніх двох-трьох років, – це зростання Китаю...вони працюють більше як професійна розвідувальна служба, ніж оператори «розбою і грабежів», яких ми бачили в минулому»[39]).

Китай уже давно є однією з найбільших цифрових загроз для Сполучених Штатів. У квітні 2021 р. найвищі посадові особи американської розвідки надали свою оцінку світових загроз, що зачіпають інтереси США, зосередившись на кібербезпеці й військових загрозах із боку Пекіна й Москви, а також на загрозі внутрішнього й міжнародного тероризму. Директори Національної розвідки, ЦРУ, АНБ, ФБР та Управління оборонної розвідки охарактеризували Китай як близького конкурента, який кидає виклик Сполученим Штатам на багатьох аренах, водночас дома-

[35] @SecBlinken [Secretary Antony Blinken] (2021). United States government official, July 19, 2021, available at: https://twitter.com/secblinken/status/1417103602133479429. (accessed March 10, 2022).

[36] Reuters (2021). U.S. charges four Chinese nationals charged in global hacking campaign. *Reuters*, July 19, 2021, available at: https://www.reuters.com/technology/four-chinese-nationals-charged-global-hacking-campaign-us-justice-department-2021-07-19/ (accessed March 10, 2022).

[37] Parker, C. B. (2018). China Exerting „Sharp Power" Influence On American Institutions. *HOOVER*, Dec. 19, 2018 available at: https://www.hoover.org/news/china-exerting-sharp-power-influence-american-institutions (accessed March 10, 2022).

[38] Там само.

[39] Wolfe, D. (2021). How China Became a Digital Adversary and Threat to the U.S. GSIExchange, July 21.2021, available at: https://gsiexchange.com/how-china-became-a-digital-adversary-and-threat-to-the-u-s/ (accessed March 10, 2022).

гаючись перегляду глобальних норм таким чином, щоб сприяти авторитарній китайській системі й що Пекін здійснює «епохальний геополітичний зсув», який відбувся на його користь за рахунок Сполучених Штатів[40].

Американське розвідувальне співтовариство сформувало свою позицію щодо Китаю як системного джерела потенційних загроз, пов'язаних із реалізацією цією країною власної стратегії, яка «заходить на територію» національних інтересів США. У звіті щодо стану загроз у світовому масштабі, опублікованому в 2021 р., Китай оцінюється як джерело «результативної й ефективної» загрози кібершпигунства. Зростаюча загроза кібернетичного впливу з боку Китаю збільшує загрози кібератак на США, обмеження американського веб-контенту, який розглядається Пекіном в якості загрози ідеологічному контролю всередині Китаю й розширенню інформаційно-технологічного авторитаризму в світі. При цьому конкретизовано такі основні кіберзагрози з боку Китаю[41]:

- Китай може здійснювати кібератаки, які, щонайменше, здатні спричинити локалізовані тимчасові порушення роботи критичної інфраструктури в Сполучених Штатах;
- Китай – світовий лідер із застосування систем спостереження й цензури для моніторингу свого населення й придушення інакомислення, особливо серед етнічних меншин, таких як уйгури;
- Пекін здійснює кібер-атаки, які впливають на громадян США й інших держав, серед яких – хакерство журналістів, крадіжка особистої інформації, блокування засобів для вільного висловлювання в інтернеті. Це – частина зусиль щодо спостереження за уявними загрозами владі КПК та адаптації зусиль щодо впливу;
- Пекін використав свою участь у глобальних зусиллях із боротьби з COVID-19 для експорту своїх інструментів і технологій спостереження;
- операції з кібершпигунства в Китаї включали компрометацію телекомунікаційних фірм, постачальників керованих послуг і поширеного програмного забезпечення, а також інших цілей, що створює можливості для потенційного збору розвідувальної інформації, атак або операцій впливу.

За останні роки з'явилося достатньо ознак того, що Китай започаткував нову політику в сфері кібератак, змістивши фокус із використання кібершпигунства на користь державним компаніям до орієнтації на цілі національної безпеки. Наприклад, китайські спеціалісти в сфері кібербезпеки повинні протягом двох днів повідомляти державу про виявлені ними «діри» в захисті інформаційних систем, такі як «нульові дні», використані для атаки на Microsoft Exchange. Вже в 2016 р. влада раптово закрила найвідомішу приватну платформу Китаю для звітності про нульові дні й заарештувала її засновника[42]. Через два роки китайська поліція оголосила, що почне виконувати закони, що забороняють «несанкціоноване розкриття» вразливостей. Того ж року китайські хакери, які регулярно були присутні на великих західних хакерських конгресах, перестали з'являтися навіть на запрошення[43]. Фактично китайська держава взяла хакерську діяльність під повний державний контроль.

За словами Дж. Курца, виконавчого директора компанії з кібербезпеки CrowdStrike, «якщо вони продовжуватимуть підтримувати цей рівень доступу з контролем, який у них є, їхня розві-

[40] Neumann, S. (2021). Intelligence Chiefs Say China, Russia Are Biggest Threats To U.S. *NPR*, April 14, 2021, available at: https://www.npr.org/2021/04/14/987132385/intelligence-chiefs-say-china-russia-are-biggest-threats-to-u-s (accessed March 10, 2022).

[41] DNI (2021). Annual Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence, April 9, 2021, available at: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf (accessed March 10, 2022).

[42] The Wall Street Journal (2016). China's 'White-Hat' Hackers Fear Dark Times After Community Founder Is Detained. *The Wall Street Journal*, August 1, 2016, available at: https://www.wsj.com/articles/BL-CJB-29440 (accessed March 10, 2022).

[43] Cyberscoop (2018). China's government is keeping its security researchers from attending conferences. *Cyberscoop*, March 8, 2018. available at: https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/ (accessed March 10, 2022).

дувальна спільнота виграє... Це гонка озброєнь у кіберпросторі» (цит. за Д. Вольфе[44]).

Позиція Китаю в кіберпротистоянні зі США

Китай завжди заперечував свою причетність до кібератак, навпаки, звинувачуючи США в організації злочинності й шпигунства в кіберпросторі. Так, у відповідь на серію виступів американських офіційних осіб, які з початком каденції Дж. Байдена оголосили Китай серед головних джерел кіберзагроз, китайські джерела називають США «провідною світовою шпигунською імперією з масовими злочинами в кіберпросторі»[45]. Нову жорстку американську політику кібербезпеки в Китаї пояснюють спробами «стримати Китай і в рамках своїх невпинних зусиль сформувати антикитайський хор серед своїх основних союзників», для чого «адміністрація Байдена прагне перетворити кіберпростір на нове поле бою, об'єднавшись зі своїми союзниками, щоб звинуватити Китай у проведенні кібератак у всьому світі»[46].

Усі американські звинувачення Китаю в сприянні кіберзлочинності й кібершпигунстві негайно засуджуються китайськими дипломатами, а також певними експертами, які натомість стверджують, що Китай завжди був довгостроковою жертвою кібератак США. В тому ж дусі заперечуються звинувачення й з боку НАТО, Європейського Союзу, Австралії, Великої Британії, Канади, Японії, Нової Зеландії При цьому лунають заклики припинити критикувати Китай на цю тему, оскільки нібито США самі тривалий час були організатором кібератак.

Звинувачуючи в організації кібератак, передусім, ЦРУ, китайські посадовці посилаються на певні інтернет-дослідження, які буцімто доводять, що США стоять за хакерською діяльністю, спрямованою на аерокосмічний сектор Китаю, науково-дослідні установи, інтернет-компанії, нафтову промисловість і державні установи. Так, Qihoo, основний постачальник послуг кібербезпеки, чиї дослідження, як правило, використовують для розуміння цифрової безпеки Китаю, повідомив, що Центральне розвідувальне управління США спрямувало кібератаки на авіаційний та енергетичний сектори Китаю, науково-дослідні організації, інтернет-компанії й урядові установи. Також зазначається, що злам міг бути спрямований на відстеження «маршруту подорожей важливих осіб»[47].

Звинувачення в кібератаках, висунуті на адресу Пекіна американськими компаніями, що викладаються звітах на зразок згаданих вище, містять значну кількість даних. Зовсім недавно китайські компанії почали робити те ж саме щодо іноземних хакерських груп. Потрібно зазначити, що Сполучені Штати рідко коментують, коли їх звинувачують у кібершпигунстві.

Риторика китайських посадовців у зв'язку з американськими звинуваченнями на адресу їхньої країни різко негативна. Так, речник міністерства закордонних справ Китаю Чжао Ліцзянь заявив, що ці звинувачення «є абсолютно неприйнятними, оскільки вони виходять з політичних цілей з метою наклепу та стримування Китаю», й що така позиція США може призвести до погіршення китайсько-американських відносин, які можуть перейти до нового мінімуму[48].

Китайська влада заявляє про те, що протягом багатьох років Китай був основною жертвою кібератак. Згідно зі щорічним звітом Національної технічної групи з реагування на надзвичайні ситуації / координаційного центру Китаю (CNCERT/CC), у 2020 р. близько 5,31 млн хостів на материковій частині Китаю контролювали загалом близько 52000 закордонних серверів ке-

[44]Wolfe, D. (2021). How China Became a Digital Adversary and Threat to the U.S. GSIExchange, July 21, 2021, available at: https://gsiexchange.com/how-china-became-a-digital-adversary-and-threat-to-the-u-s/ (accessed March 10, 2022).

[45] Qingqing, Ch., Siqi C. (2021). US turns cyberspace into another anti-China battlefield, 'futile to contain Beijing'. *Global Times*, July 20, 2021, available at: https://www.globaltimes.cn/page/202107/1229168.shtml (accessed March 10, 2022).

[46] Там само.

[47] Satter, R. (2020). Chinese cybersecurity company accuses CIA of 11-year-long hacking campaign. *Reuters*, March 3, 2020, available at: https://www.reuters.com/article/us-china-usa-cia-idUSKBN20Q2SI (accessed March 10, 2022).

[48]MFA of the PRC (2021b). Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on July 29, 2021, July 29, 2021, available at: https://www.mfa.gov.cn/ce/cohk//eng/Topics/fyrbt/t1896083.htm (accessed March 10, 2022).

рування шкідливими програмами, а трійка найбільших джерел закордонних серверів за кількістю скомпрометованих китайських хостів – усі з країн-членів НАТО[49].

Відома антивірусна компанія Antiy Labs опублікувала документ, у якому стверджує, що з 2000 р. США вже проводили масштабні атаки на глобальному рівні, – Equation, підрозділ Агентства національної безпеки (АНБ), зламав важливі інтернет-цілі в усьому світі, й що Сполучені Штати мають найбільший у світі арсенал атак у кіберпросторі, включаючи високорівневий шкідливий код, а також велику кількість нерозкритих інструментів використання вразливостей і платформ для атак[50]. За даними китайської компанії, США проникають в інформаційні системи й атакують китайського телекомунікаційного гіганта Huawei, а також країни, якщо вони купують продукцію Huawei. Також стверджується, що США використовують масову хакерську діяльність для того, щоб атакувати низку країн, включаючи Китай, із метою отримання розвідданих.

Китайський технологічний гігант 360 Security Technology повідомляв про серію атак на китайські аерокосмічні, науково-дослідні установи, нафтову промисловість і великі інтернет-компанії, здійснені хакерською організацією, пов'язаною з ЦРУ. Компанія нібито знайшла докази того, що хакерська група, APT-C-39 належить ЦРУ, і злам, простежений з 2008 р., в основному спрямований на організації в Пекіні, південнокитайській провінції Гуандун і східнокитайській провінції Чжецзян[51].

У Китаї пояснюють загострення конкуренції зі США в сфері кібербезпеки тим, що Америка намагається зберегти свою гегемонію в світі. Особливо це питання загострилось із приходом адміністрації Байдена, коли з боку Китаю розпочалась масштабна й системна інформаційна кампанія, у якій кібер-діяльність і звинувачення Пекіна як джерела кіберзагроз розглядаються як елемент загальної гри з боку США задля формування антикитайського альянсу, спрямованого на відродження американської гегемонії. Державні ЗМІ Китаю пояснили перший закордонний візит президента Джо Байдена до Європи в червні 2021 р. тим, що «старий міжнародний порядок після Другої світової війни, очолюваний США, стає все більш нежиттєздатним, а новий світовий порядок ще далекий від встановлення, оскільки глобальна система переходить від однополярної до багатополярної»[52].

Фактично можна говорити про наявність у Китаю чіткого власного уявлення про зміну світового порядку, що впливає на зовнішню орієнтацію Пекіна в епоху Байдена. В Китаї фіксують зміни в зовнішньополітичній стратегії США як такі, що становлять загрозу через те, що адміністрація Байдена розширює політичну траєкторію Вашингтона, визначаючи «більш наполегливий і авторитарний Китай» як «єдиного конкурента, потенційно здатного поєднати свою економічну, дипломатичну, військову й технологічну силу, щоб кинути постійний виклик стабільній і відкритій міжнародній системі»[53]. Як зазначають китайські спостерігачі, незважаючи на деякі можливості для співпраці, політика Байдена в Китаї схиляється до «стратегічної конкуренції і навіть конфронтації» [54].

---

[49]MFA of the PRC (2021a). Spokesperson of the Chinese Mission to the EU Speaks on a Question Concerning the Statements from the EU and NATO on the So-called Chinese Malicious Cyber Activities, July 20, 2021, available at: https://static.poder360.com.br/2021/07/nota-china-ataques-hackers.pdf (accessed March 10, 2022).

[50]*Equation Group (2017). The Analysis of Equation Drug –the Fourth Analysis Report of Equation Group, January 26, 2017, available at: https://www.antiy.net/p/the-analysis-of-equation-drug-the-fourth-analysis-report-of-equation-group/ (accessed March 10, 2022).*

[51]Blogs.360 (2019). The CIA Hacking Group (APT-C-39) Conducts Cyber-Espionage Operation on China's Critical Industries for 11 Years. 360 Core Security, available at: https://blogs.360.cn/post/APT-C-39_CIA_EN.html (accessed March 10, 2022).

[52]Qingqing, Ch., Keyue, Xu and Yelu, Xu (2021). US Turning G7 Into Anti-China, Anti-Russia Chorus 'Wishful Thinking. *Global Times*, June 6, 2021, available at: https://www.globaltimes.cn/page/202106/1225524.shtml (accessed March 10, 2022).

[53] The White House (2021). Renewing America's Advantages: Interim National Security Strategic Guidance, March 20, 2021, available at: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf (accessed March 10, 2022).

[54] Guozhu, L. (2021). "**拜登政府国家安全**战略的基本方针与发展方向, (Bài dēng zhèngfǔ guójiā ānquán zhànlüè de jīběn fāngzhēn yǔ fāzhǎn fāngxiàng/ The main policy and direction of development of the National Security Strategy of the Biden administration)". *Dangdai Shijie*, 5 (2021), pp. 50–57, available at: https://webcache.googleusercontent.com/search?q=cache:7-

У Китаї вважають, що на відміну від односторонньої позиції Трампа з відвертими нападами на Компартію Китаю, Байден обрав альтернативні інструменти багатосторонності й взаємодії з союзниками для досягнення стратегічної мети – обмеження впливу Китаю. За словами держсекретаря Тоні Блінкена, перші американо-китайські переговори у березні 2021 р. продемонстрували зростаючі тертя щодо прав людини, Тайваню, кібербезпеки й «економічного примусу до наших союзників»[55]. І вже в квітні 2021 р. Акт Сенату США про стратегічну конкуренцію свідчив про консенсус двох партій в питанні більш жорсткої стратегії щодо Китаю. В основі такої стратегії – констатація того, що «Китайська Народна Республіка використовує свою політичну, дипломатичну, економічну, військову, технологічну й ідеологічну владу, щоб стати стратегічним глобальним конкурентом для Сполучених Штатів. Політика, яку КНР дедалі частіше проводить у цих сферах, суперечить інтересам і цінностям Сполучених Штатів, їхніх партнерів і більшої частини решти світу», і що така китайська політика «поставить під загрозу майбутній мир, процвітання й свободу міжнародного співтовариства в найближчі десятиліття»[56].

У такому контексті Пекін інтерпретує посилення американської політики кібербезпеки щодо Китаю як «нову зброю США» у формуванні міжнародного фронту задля стримування Китаю. У зв'язку з цим можна навести слова Лі Хайдуна, професора Інституту міжнародних відносин Китайського університету закордонних справ: «Байден знайомий з такою тактикою «формування альянсу» в протистоянні з Китаєм. Наприклад, раніше він намагався створити альянс щодо вакцин, альянс щодо зміни клімату, альянс безпеки тощо. Звинувачення в кібератаках додають деякі нові елементи до такої тактики»[57]. Цінь Ань, керівник Пекінського Інституту кіберпросторової стратегії, зазначив, що США використовують старі прийоми для стримування Китаю, оскільки Байден хоче показати своїм союзникам, що США все ще лідирують у світі. «Байден також хоче довести американцям, що він кращий за Трампа»[58].

Пекін насторожено сприймає поширення американського підходу щодо Китаю в аспекті кібербезпеки на союзників США. Так, на саміті НАТО в червні 2021 р. Джо Байден і партнери по НАТО наголосили на загрозах безпеці, які надходять із боку Китаю й Росії, а в комюніке Альянсу містилася теза про стримування Китаю, що можна розглядати як зміни в стратегії НАТО. У зв'язку з цим МЗС Китаю засудило цей крок як перетворення кіберпростору на нове поле бою шляхом уведення військового альянсу в кіберпростір, а речник зовнішньополітичного відомства КНР заявив, що «це не буде корисним для підтримки власної безпеки, але спровокує гонку озброєнь у кіберпросторі, посилить конфлікти між країнами в інтернеті й поставить під загрозу мир і безпеку»[59].

Висновки. Кібернетичні загрози зростають випереджаючими темпами порівняно з усіма іншими проблемами, що пов'язані з розвитком кіберпростору. Сьогодні світовими лідерами в кіберсфері й секторі інформаційної (кібер) безпеки є США й Китай. Сполучені Штати залиша-

mexZ_mX1EJ:https://dysw.cnki.net/kcms/detail/detail.aspx%3Ffilename%3DJSDD202105008%26dbcode%3DCJFD%26dbname%3DCJFD2021%26v%3D+&cd=1&hl=uk&ct=clnk&gl=ua (accessed March 10, 2022).

[55] US Department of State (2021). Secretary Antony J. Blinken, National Security Advisor Jake Sullivan, Director Yang and State Councilor Wang at the Top of Their Meeting. Anchorage, March 18, 2021, available at: https://www.state.gov/secretary-antony-j-blinken-national-security-advisor-jake-sullivan-chinese-director-of-the-office-of-the-central-commission-for-foreign-affairs-yang-jiechi-and-chinese-state-councilor-wang-yi-at-th/ (accessed March 10, 2022).

[56] US Senate Committee on Foreign Relations (2021). Strategic Competition Act of 2021, April 2021.

[57] Qingqing, Ch., Siqi C. (2021). US turns cyberspace into another anti-China battlefield, 'futile to contain Beijing'. *Global Times*, July 20, 2021, available at: https://www.globaltimes.cn/page/202107/1229168.shtml (accessed March 10, 2022).

[58] National Cyber Security News. Today (2021). US turns cyberspace into another anti-China battlefield, 'futile to contain Beijing'. *National Cyber Security News*. Today, July 28, 2021, available at: https://nationalcybersecuritynews.today/us-turns-cyberspace-into-another-anti-china-battlefield-futile-to-contain-beijing-cybersecurity-cyberattack/ (accessed March 10, 2022).

[59] MFA of the PRC (2021b). Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on July 29, 2021, July 29, 2021, available at: https://www.mfa.gov.cn/ce/cohk//eng/Topics/fyrbt/t1896083.htm (accessed March 10, 2022).

ються безумовним світовим лідером у сфері кібербезпеки, але Китай швидко скорочує своє відставання, спираючись на потужний потенціал людських і економічних ресурсів в кіберсфері.

Сторони звинувачують одна одну в кібератаках з економічною метою, кібершпигунстві, а протягом останніх років – і в політично мотивованих діях проти інформаційних систем. Незважаючи на спроби узгодити політики в цій сфері, напруженість між США й Китаєм у зв'язку з нарощенням кіберпотенціалу зростає. У США констатують зміну стратегії кібератак з боку Китаю в напрямі від звичайного кібершпигунства до переслідування політичних і безпекових цілей і перебирання системного контролю над джерелами кіберзагроз через безпекові структури КНР.

Китай звинувачує США у використанні кіберінструментів для посилення гегемонії в світі й перенесенні кіберзагроз в сферу гонки озброєть. При цьому офіційний Пекін наполягає на реалізації власної стратегії досягнення «багатополярного» світу, негативно сприймаючи зусилля адміністрації Джо Байдена щодо консолідації країн Заходу перед кіберзагрозами з боку Китаю. За нової адміністрації США напруження у відносинах з Китаєм у кіберсфері посилилося й зберігалося на значному рівні принаймні до початку збройної агресії РФ проти України[60]. Проте ймовірно, що ця ситуація зазнає змін. Про це можна говорити, посилаючись на офіційні повідомлення про «стратегію президента Байдена щодо Китаю, в якій чиновники дійшли до висновку, що не можуть змінити поведінку Пекіна»[61].

Очевидно, що сфера кібербезпеки у відносинах між США й Китаєм стає все більш актуальною в аспекті стратегій безпеки цих обох світових лідерів. Кожен з них використовує інструмент кібернетичного впливу також як засіб для здійснення стратегічних комунікацій на рівні відносин зі стратегічними партнерами. Тому ці питання набуватимуть усе більшої ваги з точки зору дослідницьких інтересів, зокрема щодо реалізації зовнішньополітичних інтересів у відносинах із країнами.

References

1. Atlantic Council (2013). Chinese Army unit is seen as tied to hacking against U.S. *Atlantic Council*, February 19, 2013, available at: https://www.atlanticcouncil.org/blogs/natosource/chinese-army-unit-is-seen-as-tied-to-hacking-against-us/ (accessed March 10, 2022).

2. Austin, G. (2015). No Easy Solutions in U.S.-China Cyber Security. *East Asia Forum*, October 6, 2015.

3. BBC (2014). US justice department charges Chinese with hacking. *BBC*, 14 May, 2014, available at: https://www.bbc.com/news/world-us-canada-27475324 (accessed March 10, 2022).

4. Blogs.360 (2019). The CIA Hacking Group (APT-C-39) Conducts Cyber-Espionage Operation on China's Critical Industries for 11 Years. 360 Core Security, available at: https://blogs.360.cn/post/APT-C-39_CIA_EN.html (accessed March 10, 2022).

5. Brown, G., Yung, C. D. (2017b). Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace. *The Diplomat*, January 19, 2017, available at: https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/ (accessed March 10, 2022).

6. Brown, G., Yung, C. D. (2017). Evaluating the US-China Cybersecurity Agreement, Part 3: Over a year later, what impact has the 2015 cyber agreement had on U.S.-China relations? *The Diplomat*, January 21, 2017, available at: https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/ (accessed March 10, 2022).

7. Carr, J. (2015). Cyber Attacks: Why Retaliating Against China Is the Wrong Reaction. *The Diplomat*, August 6, 2015.

8. Chang, A. (2015). *Warring State: China's Cybersecurity Strategy.* Washington, D.C.: Center for a New American Security, December 2015, p. 7 and 10.

[60] Kharpal, A. (2022). China state-backed hackers compromised networks of at least 6 U.S. state governments, research finds. *CNBC*, March 9, 2022, available at: https://www.cnbc.com/2022/03/09/china-state-backed-hackers-compromised-6-us-state-governments-report.html (accessed March 10, 2022).

[61] Wong, E., Swanson, A. (2022). U.S. Aims to Constrain China by Shaping Its Environment, Blinken Says. *The New York Times*, May 26, 2022, available at: https://www.nytimes.com/2022/05/26/us/politics/china-policy-biden.html (accessed My 30, 2022).

9. China's 'White-Hat' Hackers Fear Dark Times After Community Founder Is Detained. *The Wall Street Journal*, 1 Aug. 2016. URL: https://www.wsj.com/articles/BL-CJB-29440.

10. China's government is keeping its security researchers from attending conferences. *Cyberscoop*, Mar. 8, 2018. URL: https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/.

11. Chong, J. (2010). Cyber: The Invisible New Battlefront [Wangluo: Kanbujian de xin zhanxian], *Seeking Truth* [Qiu Shi], No. 13, 2010, p. 53–55.

12. Cyberscoop (2018). China's government is keeping its security researchers from attending conferences. *Cyberscoop*, March 8, 2018. available at: https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/ (accessed March 10, 2022).

13. Deibert, R. (2015). Trajectories for Future Cybersecurity Research. *The Oxford Handbook of International Security.* Ed. by A. Gheciu and W. C. Wohlforth. Oxford: Oxford University Perss, p. 531-556.

14. Diamond, L., Carson, B. (2019). Jaw-Jaw: How Chinese Sharp Power Takes Aim at American Democracy. *War on the Rocks.* [online], February 5, 2019, available at: https://warontherocks.com/ 2019/02/jaw-jaw-how-chinese-sharp-power-takes-aim-at-american-democracy (accessed March 10, 2022).

15. DNI (2021). Annual Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence, April 9, 2021, available at: https://www.dni.gov/files/ODNI/ documents/assessments/ATA-2021-Unclassified-Report.pdf (accessed March 10, 2022).

16. Equation Group (2017). The Analysis of Equation Drug –the Fourth Analysis Report of Equation Group, January 26, 2017, available at:https://www.antiy.net/p/the-analysis-of-equation-drug-the-fourth-analysis-report-of-equation-group/ (accessed March 10, 2022).

17. Finkle, J. (2012). Hundreds more cyber attacks linked to 2009 Google breach. *Reuters*, Sept. 12, 2012, available at: https://www.reuters.com/article/cybersecurity-espionage-idUSL2E8K7A9E 20120907 (accessed March 10, 2022).

18. Fireyes (2013). *Cyber Threat Intelligence on Advanced Attack Groups and Technology Vulnerabilities.* Threat Intelligence Reports. Fireyes, 2013.

19. Greenberg, A. (2017). China tests the limits of its U.S. hacking truce. *Wired*, October 13, 2017, available at:https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/# (accessed March 10, 2022).

20. Guozhu, L. (2021). "**拜登政府国家安全**战略的基本方针与发展方向, (Bài dēng zhèngfǔ guójiā ānquán zhànlüè de jīběn fāngzhēn yǔ fāzhǎn fāngxiàng/ The main policy and direction of development of the National Security Strategy of the Biden administration)". *Dangdai Shijie*, 5 (2021), pp. 50–57, available at: https://webcache.googleusercontent.com/search?q=cache:7-mexZ_mX1EJ:https://dysw.cnki.net/kcms/detail/detail.aspx%3Ffilename%3DJSDD202105008%26dbcode%3DCJFD%26dbname%3DCJFD2021%26v%3D+&cd=1&hl=uk&ct=clnk&gl=ua (accessed March 10, 2022).

21. Harold, S. W., Libicki, M. C., & Cevallos, A. S. (2016). The "Cyber Problem" in U.S.-China Relations. In *Getting to Yes with China in Cyberspace* (pp. 1–16). RAND Corporation, available at: http://www.jstor.org/stable/10.7249/j.ctt1cx3vfr.6 (accessed March 10, 2022).

22. IISS (2021). Cyber Capabilities and National Power: A Net Assessment. *IISS. Research Papers*, June 28, 2021, available at: https://www.washingtonpost.com/politics/2021/06/28/ cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/ (accessed March 10, 2022).

23. Julian N. (2021). United States' and China's Cybersecurity Policies: Collaboration or Confrontation? *Journal of International Relations*, January 24, 2021, available at: http://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation (accessed March 10, 2022).

24. Kharpal, A. (2022). China state-backed hackers compromised networks of at least 6 U.S. state governments, research finds. *CNBC*, March 9, 2022, available at: https://www.cnbc.com/ 2022/03/09/china-state-backed-hackers-compromised-6-us-state-governments-report.html (accessed March 10, 2022).

25. Lieberthal, K. (2012) *Cybersecurity and U.S. – China Relations*. Jonh L. Torton China Institute in Brookings. 52 p., available at: https://www.brookings.edu/wp-content/uploads/ 2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf (accessed March 10, 2022).

26. Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. *International Security*, Vol. 39. №. 3, p. 7-47.

27. Linfei, Zh. (2015). Commentary: U.S. Should Think Twice Before Retaliating Against China over Unfounded Hacking Charges. *Xinhua.* August 3, 2015.

28. Mandiant Consulting Services (2013). APT1: Exposing One of China's Cyber Espionage Units, 2013, available at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (accessed March 10, 2022).

29. MFA of the PRC (2021a). Spokesperson of the Chinese Mission to the EU Speaks on a Question Concerning the Statements from the EU and NATO on the So-called Chinese Malicious Cyber Activities, July 20, 2021, available at: https://static.poder360.com.br/2021/07/nota-china-ataques-hackers.pdf (accessed March 10, 2022).

30. MFA of the PRC (2021b). Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on July 29, 2021, July 29, 2021, available at: https://www.mfa.gov.cn/ce/cohk//eng/Topics/fyrbt/t1896083.htm

31. Morgan, S. (2021). *2021 Report: Cyberwarfare in the C-suite*, Cybersecurity Ventures, available at:https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf (accessed March 10, 2022).

32. National Cyber Security News. Today (2021). US turns cyberspace into another anti-China battlefield, 'futile to contain Beijing'. *National Cyber Security Ne*ws. *Today*, July 28, 2021, available at: https://nationalcybersecuritynews.today/us-turns-cyberspace-into-another-anti-china-battlefield-futile-to-contain-beijing-cybersecurity-cyberattack/ (accessed March 10, 2022).

33. Neumann, S. (2021). Intelligence Chiefs Say China, Russia Are Biggest Threats To U.S. *NPR*, April 14, 2021, available at: https://www.npr.org/2021/04/14/987132385/intelligence-chiefs-say-china-russia-are-biggest-threats-to-u-s (accessed March 10, 2022).

34. Parker, C. B. (2018). China Exerting „Sharp Power" Influence On American Institutions. *HOOVER*, Dec. 19, 2018 available at: https://www.hoover.org/news/china-exerting-sharp-power-influence-american-institutions (accessed March 10, 2022).

35. Perlroth, N. (2021). How China Transformed Into a Prime Cyber Threat to the U.S. *The New York Times*, July 19, 2021, available at: https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html (accessed March 10, 2022).

36. Qingqing, Ch., Keyue, Xu and Yelu, Xu (2021). US Turning G7 Into Anti-China, Anti-Russia Chorus 'Wishful Thinking. *Global Times,* June 6, 2021, available at: https://www.globaltimes.cn/page/202106/1225524.shtml (accessed March 10, 2022).

37. Qingqing, Ch., Siqi C. (2021). US turns cyberspace into another anti-China battlefield, 'futile to contain Beijing'. *Global Times*, July 20, 2021, available at: https://www.globaltimes.cn/page/202107/1229168.shtml (accessed March 10, 2022).

38. Reuters (2021). U.S. charges four Chinese nationals charged in global hacking campaign. *Reuters*, July 19, 2021, available at: https://www.reuters.com/technology/four-chinese-nationals-charged-global-hacking-campaign-us-justice-department-2021-07-19/ (accessed March 10, 2022).

39. Satter, R. (2020). Chinese cybersecurity company accuses CIA of 11-year-long hacking campaign. *Reuters*, March 3, 2020, available at: https://www.reuters.com/article/us-china-usa-cia-idUSKBN20Q2SI (accessed March 10, 2022).

40. Schaffer, A. (2021). The Cybersecurity 202: The United States is still number one in cyber capabilities. *The Washington Post*, June 28, 2021., available at: https://www.washingtonpost.com/ politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/ (accessed March 10, 2022).

41. Soo, Z. (2019). How Huawei beat America's anti-China 5G propaganda war in Southeast Asia, years before it even began. *South China Morning Post*, April 22, 2019, available at: https://www.scmp.com/tech/article/3006935/how-huawei-beat-americas-anti-china-5g-propaganda-war-southeast-asia-years-it (accessed March 10, 2022).

42. Swaine, M, D. (2013). Chinese Views of Cybersecurity in Foreign Relations. *China Leadership Monitor,* No. 42, fall 2013.

43. The Wall Street Journal (2016). China's 'White-Hat' Hackers Fear Dark Times After Community Founder Is Detained. *The Wall Street Journal*, August 1, 2016, available at: https://www.wsj.com/articles/BL-CJB-29440 (accessed March 10, 2022).

44. The New York Times (2015). Obama and Xi Jinping of China Agree to Steps on Cybertheft. *The New York Times*, September 25, 2015, available at: https://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html (accessed March 10, 2022).

45. The White House (2021). *Renewing America's Advantages: Interim National Security Strategic Guidance*, March 2021, 20, available at: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf (accessed March 10, 2022).

46. US Department of State (2021). Secretary Antony J. Blinken, National Security Advisor Jake Sullivan, Director Yang and State Councilor Wang at the Top of Their Meeting. Anchorage, March 18, 2021, available at: https://www.state.gov/secretary-antony-j-blinken-national-security-advisor-jake-sullivan-chinese-director-of-the-office-of-the-central-commission-for-foreign-affairs-yang-jiechi-and-chinese-state-councilor-wang-yi-at-th/ (accessed March 10, 2022).

47. US Senate Committee on Foreign Relations (2021). Strategic Competition Act of 2021, April 2021.

48. Wenli, Yi, (2012). Divergence Between China and the U.S. and the Path Toward Cooperation in Cyberspace ["Zhong-Mei zai Wangluo Kongjian de Fenqi yu Hezuo Lujing"]. *Contemporary International Relations* [Xiandai Guoji Guanxi], Vol. 22, No. 4, July/August 2012, p. 124–141.

49. Wolfe, D. (2021). How China Became a Digital Adversary and Threat to the U.S. *GSIExchange*. July 21, 2021, available at: https://gsiexchange.com/how-china-became-a-digital-adversary-and-threat-to-the-u-s/ (accessed March 10, 2022).

50. Wong, E., Swanson, A. (2022). U.S. Aims to Constrain China by Shaping Its Environment, Blinken Says. *The New York Times*, May 26, 2022, available at: https://www.nytimes.com/2022/05/26/us/politics/china-policy-biden.html (accessed My 30, 2022).

51. Xinming, M. (2015). What Kind of Internet Order Do We Need? *Chinese Journal of International Law*, Vol. 14. No. 2, 2015, p. 399–403.

52. Zetter, K. (2013). New York Times Hacked Again, This Time Allegedly by Chinese. *Wired*, January 31, 2013, available at: https://www.wired.com/2013/01/new-york-times-hacked/ (accessed March 10, 2022).

53. @SecBlinken [Secretary Antony Blinken] (2021). United States government official, July 19, 2021, available at: https://twitter.com/secblinken/status/1417103602133479429 (accessed March 10, 2022).