Centre for Defence and Security Strategic Studies &
Interdisciplinary Doctoral School,
"Carol I" National Defence University

DOI: 10.53477/3045-2309-25-13

THE THIRD AND THE FOURTH DEPARTMENTS OF THE PEOPLE'S LIBERATION ARMY AND CYBER THREATS

Alida Monica Doriana BARBU, PhD,
PhD Candidate in International Relations and Security Studies,
Babes-Bolyai University, Cluj-Napoca, Romania.
E-mail: alida.barbu7@gmail.com

Abstract: *The Chinese Communist Party and the People's Liberation Army have been interested in war and electronic espionage since the third decade of the last century, when Deng Xiaoping was establishing technical units in military bases in southern China. The purpose of this study is to determine which strategies are being used by The People's Republic of China to gain advantage over other states and how effective they are, as well as the manner in which they are perceived by the USA, EU and Romania. The current paper aims to provide an understanding of the way in which the People's Liberation Army conducts information, psychological, electronic, cyber and meta warfare to help a competing China to access and preserve power. The development of specialized literature on China's hostile capabilities has the effect of increasing security culture among the Euro-Atlantic and Romanian public and possibly deterring China. In order to achieve its purpose, the following methodology was used: reviewing specialized literature, qualitative research, and testing Charles Tilly's theory - war made the state and the state made war − because state institutions and war preparation are mutually reinforced (bellum est pater omnium).*

Keywords*: Chinese military espionage; Chinese cyber warfare; 3rd and 4th Departments of People's Liberation Army; INEW (Integrated Network Electronic Warfare); Meta War; China-Romania relations.*

Introduction

The cyber domain is recognized by the PRC as a critical area for national security, hence the intention to develop cyber warfare capabilities. The PLA admits that the components of IO (Information Operations) - EW (Electronic Warfare), cyber, psychological and space warfare - are necessary to achieve military superiority (Office of the Secretary of Defense 2023, 181-182). The PRC can launch cyber attacks that, at the very least, can cause localized, temporary disruptions to critical infrastructures, and the PRC believes these capabilities are even more effective against militarily superior adversaries that depend on information technologies. As a result, the PRC is advancing its cyber attack capabilities and has the ability to launch cyber attacks, evolving from the INEW to the Meta Warfare.

Since the 1950s, the Deputy Chief of Staff of the People's Liberation Army (PLA) was responsible for military intelligence sectors: PLA-2 (2nd Department of the People's Liberation Army) - *Er Bu* or *Qingbaobu*, which dealt with military espionage and PLA-3 (3rd Department of the People's Liberation Army – 1950-2016) - *San Bu*, which was in charge of military SIGINT. The system perpetuated its structure without much change, with General Chen Xiaogong, the son of a friend of Zhou Enlai, acquiring in July 2007 the position of Deputy Chief of Staff of the People's Liberation Army (PLA). In the late 1980s, Department 4 (*Si Bu* or PLA-4) was established to deal with the newly emerging electronic warfare and shared with PLA-3 the conduct of cyber warfare (Faligot 2019, 512).

In 2016, the General Staff Department was abolished following the People Liberation Army Reform. The PLA-4 functions were taken over by the Network Systems Department of the Strategic Support Force (SSF) of the PLA. The division of cyber espionage and offensive cyber forces between PLA-3 and PLA-4 did not achieve an integrated fighting force. SSF was established for a more comprehensive, integrated approach to information operations that brought the concepts of PLA doctrine and strategy up to date. SSF resembled U.S. Strategic Command (USSTRATCOM), responsible for combatant, cyber operations, space and strategic C4ISR support command, but differed by being a military service rather than a Joint Force Command. Also, the nuclear component was not among its concerns (Kania, Costello 2018, 107).

The Strategic Support Force was disbanded on 19 April 2024 and split into three independent arms: the People's Liberation Army Aerospace Force, the People's Liberation Army Cyberspace Force, and the People's Liberation Army Information Support Force (Chen 2024).

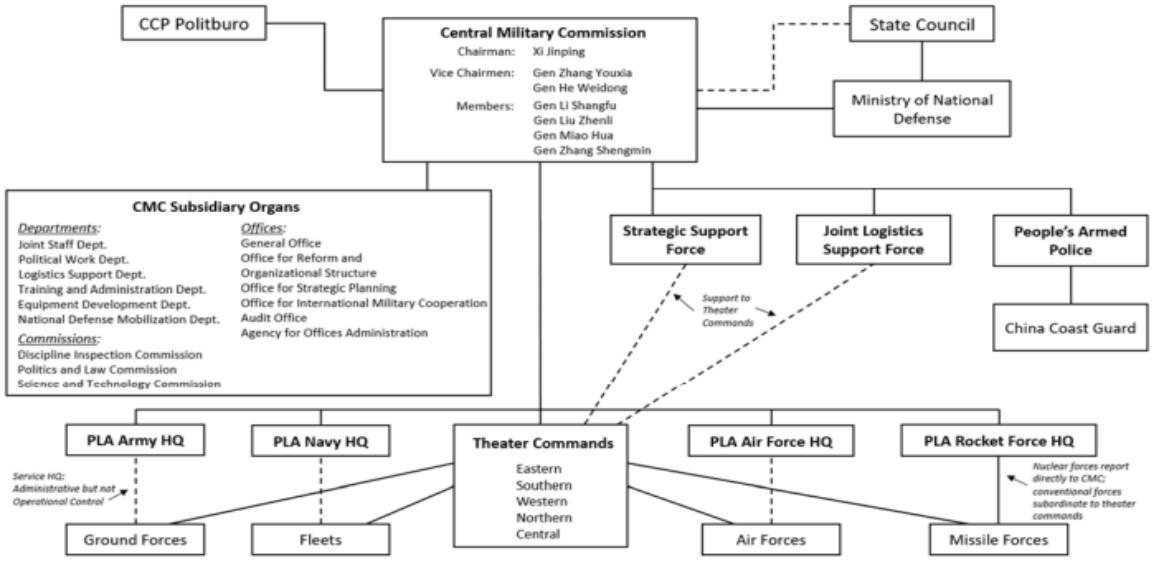

Figure no. 1: China Military Leadership Organizational Chart in 2023
(Office of the Secretary of Defense 2023, 46)

1. Chinese Military Bases all Over the World

1.1. Chinese Military Bases in the People's Republic of China

Deng Xiaoping's friend Nie Rongzhen set up a secret radio station in Hong Kong to communicate with the Comintern in Vladivostok and Harbin, while Zhou Enlai in Shanghai monitored the Kuomintang's movements. Li Kenong, who would be appointed in 1950 head of the Department of Social Affairs (DSA), the party's secret service, and at the same time hold the position of Deputy Chief of Staff of the People's Liberation Army (PLA), came to Zhou Enlai's aid by infiltrating the radio systems of the Kuomintang nationalists (Faligot 2019, 512).

The first communication school dates back to the period of the Red Army of the Chinese Workers and Peasants, with the headquarters chosen by Deng Xiaoping in Ruijin Province, Pingshangang City, in March 1933. The People's Liberation Army, the current name of the Red Army of the Chinese Workers and Peasants, celebrated in November 2006 this first school of communications, special by the impressive number (2100) of connections systems that covered the entire China, to which the Chinese Communist Party owes its long march to power (Faligot 2019, 512).

In 1950, PLA-3 numbered 20,000 technicians, intercepting the communications of foreign armies. Of the dozens of bases picking up and decoding signals from the US, Japan, Taiwan, former Soviet Muslim republics, Russia, South and North Korea, India, the most developed PLA-3 station was located in Xibeiwang District. Tibet, XinJiang and India were monitored from the Bureau of Technical Reconnaissance (BRT3) at the Chengdu station, Japan and Korea at the Shenyang station. The stations near Kunming were assigned the surveillance of Myanmar and Vietnam. New stations have been established on the Paracel Islands since the 1980s, and the Lingshui base in Hainan Island was tasked in 1995 with expanding its coverage from the Philippines and Vietnam to the entire South China Sea. The Lop Nor and Kashi stations, along with the Dingyanchen base in Xinjiang province intercepted the communications of the former Muslim Soviet republics and Russia, and the Changli base intercepted satellite communications. The Canton and Fujian military districts constantly monitored Taiwan. Each military region, be it Beijing, Canton, Lanzhou, Nanjing, Shenyang, Jinan, Chengdu, had its station (Faligot 2019, 513).

Figure no. 2: Major SIGINT stations in China (Faligot 2019, Appendix IX)

Research of academic databases and Chinese government websites by James T. Areddy and Paul Mozur of the Wall Street Journal in 2014 revealed that the organizational structure of the PLA-3 Department was almost identical to that of the NSA, with operational units throughout China. (The Wall Street Journal 2014) In 2014, more than 100,000 analysts, officers, hackers, linguists recruited from top universities, coordinated operations from military intelligence offices according to various geographical areas, including US surveillance from the Shanghai facility located in the vicinity of the transoceanic communications cables connecting the United States to China.

1.2. Chinese Military Bases Abroad

PLA-3 undertook SIGINT (Signals Intelligence) and CNO (Computer Network Operations) operations not only domestically but also abroad through its stations in North Korea, Pakistan, Djibouti, Cuba (The Economist 2023), etc. In June 2023, the Biden administration said the People's Republic of China had espionage facilities in Cuba. Wall Street Journal investigations identified four Chinese interception bases at Bejucal near Havana, Calabazar, Wajay and El Salao, east of Santiago de Cuba. The Bejucal station, built between 2010 and 2019, has the ability not only to intercept communications and track US satellites, but also to gather data on launches of SpaceX's Falcon 9 and Falcon Heavy rockets from Florida's Cape Canaveral Space Force Station and the Kennedy Space

Center, of interest to China, which wants to overtake US space launch technology. The El Salao base, still under construction, will be able to monitor the nearby US Naval Base Guantánamo Bay, the US Navy and allies operating in the South Atlantic Ocean and the Caribbean. Even though modern military communications are encrypted, data on the origin, frequency, rate, and direction of communications traffic, obtained by collecting data from high-frequency radio transmissions, is very valuable. About 10 kilometers north of Bejucal is the Wajay station, expanded over the past twenty years with 12 antennas of different orientations and sizes and a solar farm, insurance against Cuba's unreliable electricity grid. Calabazar, the SIGINT base located on the outskirts of Havana, along with Bejucal and Wajay, served as a communications facility in the 1960s, according to declassified CIA documents. Among the improvements made is the solar farm, installed since 2012, larger than the one in Wajay (The Economist 2023).

As early as 1995, China had the most extensive SIGINT network in the entire Asia-Pacific region (Stokes 1999), joining the UK, the Russian Federation and of course the US as one of the world's leading SIGINT players. Jason Pan, who worked for the Taipei Times as an intelligence investigative specialist, identified in PLA-3 in March 2015 more than 12 new bureaus dealing with online warfare (Lo, Pan 2015, 3), of which the Sixth Bureau, located on the campus of Wuhan University in Wuhan, Hubei Province, was tasked with cyber warfare against Taiwan. Interception of telecommunications signals, technical surveillance and intelligence gathering of important agencies in Taiwan, reconnaissance of satellite images against Taiwan, hacking of computers and mobile phone service networks have been identified by Taiwan's Military Intelligence Bureau (MIB) and Ministry of National Defense (MND) as Chinese espionage activities, all under the guise of non-profit foundations, academic research centers or private sector companies. PLA-3's Sixth Bureau had units of network specialists, analysts, computer technicians, and hackers working in Wuhan University offices under the guise of telecommunications labs and research centers (Lo Pan 2015, 3).

And other nations that have suffered theft of digital information from cyber attacks have reported that Chinese cyber army units operate on university campuses under the guise of academic research. In Shanghai's Pudong District, PLA Unit 61398, which was found to be hacking commercial intelligence and planning malicious attacks against the US and other Western countries, was part of PLA-3's Office 2. The unit came under the scrutiny of the US Department of Justice after on May 19, 2014, five PLA officers were indicted for economic cyber espionage against US companies, such as Alcoa, US Steel, Westinghouse Electric, Allegheny Technologies, United Steel, Service Workers International Union, Paper and Forestry, Manufacturing, Allied Industrial, Rubber, Energy. Taiwan's National Security Bureau found 7.22 million Chinese cyber attacks in 2013. The Ministry of Justice's Bureau of Investigation (MJIB) was under siege by 1.56 million cyber attacks and the Ministry of Defense 1.01 million attacks (Lo, Pan 2015, 3).

2. PLA-3 and PLA-4, Two Swords in the Same Sheath

Network-Centric Warfare (NCW) is a military doctrine that seeks to gain an advantage over the enemy by connecting all forces through information technology, using a secure communications network to integrate command and control elements, sensors and information transmission. General Deepak Sharma of the Institute for Defense Studies and Analyses from New Delhi described in the April 2010 issue of the Journal of Defense Studies (Sharma 2010, 37-38) China’s INEW Strategy (Integrated Network Electronic Warfare), the name for the offensive mission consisting of electronic warfare (EW) and computer network attacks (CNA) under the umbrella of PLA-4 (Electronic Countermeasures) of the General Staff of the People's Liberation Army. Intelligence gathering and computer network defense (The Computer Network Defense - CND) was undertaken by PLA-3 (Signals Intelligence) and militia units specialized in IW (Information Warfare) (Sharma 2010, 37-38).

The INEW concept was formulated by Major General Dai Qingmin, former head of PLA-4, who envisioned future intelligence operations to “destroy and control the enemy’s information

infrastructure and strategic vitality by selecting key enemy targets and launching electronic attacks on networks; this integration of electronic and cyber warfare was to be superior to the US military's approach" (Sharma 2010, 37-38).

China's espionage and surveillance activities against Taiwan are divided into HUMINT and SIGINT. The Ministry of State Security (Guoanbu), together with the United Workers' Front Department, which is part of the Central Committee of the Communist Party of China, conducts human intelligence programs against Taiwan, seeking to recruit Taiwanese officials and agents, while the PLA-3 monitors radar, telecommunications, radio and other signals. Between 2009-2012, as the era of Hu Jintao was waning, he was replaced by XI Jinping in 2013, the intelligence services of the PLA went through an era of technological development: submarines, drones, satellites, intelligence gathering by oceanographic ships. Didier Huguenin wrote in his Master's dissertation *Manouevres et pratiques d'Intelligence autour d'une stratégie Sud-Sud* (Faligot 2019, 545) from Université de Marne-La-Valée about Chinese espionage in the African countries of Zimbabwe, Mali, Djibouti, the Democratic Republic of Congo. ELINT (electromagnetic intelligence) and SIGINT operations were conducted under the guise of telephone service assistance. In addition to the PLA-2, PLA-3 and PLA-4 reporting to the General Staff, the Department of International Relations and military security were added which answered to the General Political Department. In the group of organizations dealing with communications and military interception, the PLA Communications Department liaised between the Central Military Commission, the units that protected the most sensitive government lines and the Army General Staff, since 2011 it was renamed the Informatization Department (Faligot 2019, 514).

In the summer of 2007, General Chen Xiaogong was appointed deputy chief of staff due to his experience in Pakistan and Afghanistan, as well as his specialization in relations with the US. PLA-3, PLA-4, but also the Department of Communications came under his supervision at a time when the suspicions of Taiwanese, Indian, Western, Korean, Japanese agencies hovered over them regarding cyber attacks targeting websites around the world. In 2009, General Yang Hui, the former deputy director of PLA-3, was appointed chief of PLA-2, promoted because of his strong knowledge of cyber warfare. It was speculated that the appointment was part of the cyberwarfare interest group's strategy to take over the military entirely (Faligot 2019, 545-546).

The cyber war took off in 2008, when the databases and websites of the Indian Ministry of External Affairs were attacked by Chinese hackers, identified by the Indian counterintelligence service through IP addresses. China's breach of India's National Security Council computer systems demonstrated the need for a cyber counter-strike force consisting of the Bureau of Economic Intelligence, the Army's CyberSecurity Establishment, the National Technology Research Organization (NTRO - the equivalent of the NSA), working with RAW. The Chinese attacks had also targeted the computer system of the Dalai Lama, who is in exile in India. It was not just Asia that had to feel threatened, but Europe and North America as well (Faligot 2019, 546).

In 2009, Chinese hackers penetrated the Gmail messaging system as a result of the trade war between Internet provider Baidu and Google. The PLA-3 was suspected of this large-scale operation, which would have been too difficult for hacker groups or civilian agencies. The Bureau of Technical Reconnaissance (BRT3) in Chengdu, which handled operations against India, Tibet and the Xinjiang region, was commended for gathering intelligence from hostile environments. The US was no less, and in 2009 carried out no less than 230 million attacks on the website of the Chinese Ministry of Defense. The FBI, with the support of the NSA arm of the US consulate in Hong Kong and Britain's GCHQ, dismantled a Chinese network in Louisiana by intercepting Hotmail, Bellsouth.net, Gmail and FedEX emails and the conversations of Kuo Tai Shen, a Chinese-American from Taiwan with Gregg Bergersen, an arms dealer to Taiwan and a US agent recruited from the Defense and Security Cooperation Agency in Arlington, Virginia, and Kang Yuxin, a Chinese national and liaison of Kuo Tai Shen. In 2009, the Northrop Grumman Corporation released its analysis of the cyber warfare techniques of the PLA-2, PLA-3, PLA-4, marking the first time that links between Chinese security

services and hacker groups were officially identified. The Hack4.com group attacked in 2008 Canada, the USA, but also the French embassy in China for the "mistake" of President Nicolas Sarkozy to shake hands in Poland with Dalai Lama during the previous month. The French secret services managed to link Guoanbu (Ministry of State Security), Gonganbu 1st Research Bureau (Ministry of Public Security) and Hack4.com, while PLA-3 was using the know-how of technical university graduates (Faligot 2019, 546-549).

3. The Meta War

Shi Zhan, Director of the World Politics Research Center at the China Foreign Affairs University, argues in his paper *The First War in the Metaverse* (Shi 2024) that a beta version of the meta-war could be considered the Russian-Ukrainian War. It is also called the first full-scale drone war, the first commercial space war, and the first AI war (Baughman 2024, 34). With network communication, such as social networks, the war has become a more personal experience field, because images from the battle can be transmitted directly to people's smartphones without the need for Without government mediation or the media, civilians become part of the war through social networks on which we shared opinions. The chatbot eVorog (eEnemy) was made available to citizens in March 2022 by the Ministry of Digital Transformation of Ukraine for reporting Russian troop movements, with the reward coming in the form of a folded arm emoji. Another option in the menu, in the form of a drop of blood, allows Ukrainians to upload images of war crimes in the area such as Bucha, Irpin, Gostomel (Bergengruen 2022).

The chatbot, accessible via smartphone, is found on the Telegram platform, and the interface uses the government app Diia to verify the identity of those uploading images and information and the location via the phone's GPS. This networked gamification for Ukrainian civilians makes them part of the war by intersecting the digital (smartphone app) and physical (perceiving Russian military operations) (Baughman 2024, 34).

PLA aims for the intelligentization of war, technological dominance can be achieved through the dual-use metaverse, both civilian, economic and military growth on the battlefield. The military term Metaverse, first appeared in November 2021 in the PLA Daily article Discovery of the Metaverse, was intended to deter conflict by describing the hours of war. Allowing civilians to experience, in real time, the traumas of war through the re-creation of war scenes by media authorities, was supposed to inoculate societies' appetite for peace. Within months, the dialogue around the metaverse in AEP has evolved towards a military metaverse or battleverse, aimed at winning the future intelligent war. The PLA articles developed ways to achieve a military metaverse and possibilities to disrupt the use of one's own metaverse by enemies (Baughman 2024, 34).

In the PLA article on the metaverse, titled *Meta-War: An Alternative*, authors Zhang Yuantao, Luo Yanxia, and You Xiaotong conceptualize future wars, highlighting how smart warfare leads to meta-war. Meta-war is defined as "a new type of military activity that uses armed confrontation to conquer the will of the adversary and achieve objectives using politics, economics, and social interaction supported by the technology of the metaverse". The combat super system integrates smart and virtual devices, brain-computer interfaces, augmented and mixed reality with the military force on the real battlefield, in a triumvirate the physical battlefield, the virtual battlefield and *the brain battlefield* - the perceptions of officers (Baughman 2024, 34).

4. Romania-China Bilateral Relations during the Presidency of Xi Jinping

Romania and China share values and cultural, diplomatic and last, but not least, economic ties. The vulnerabilities of Chinese Dahua and Hikvision cameras, bought by the Romanian institutions, as well as the cyber attacks that Romanian Members of Parliament were subjected to from APT31, a Chinese hacker group, are challenges, but not cracks in the bilateral relations.

4.1. Romania-China Bilateral Relations During the Presidency of Xi Jinping

Chinese Press highlights friendly relations between China and Romania. The article published on the 24th of January 2025 in China Briefing (Sgueglia 2025) marks the commemoration in 2024 of the 75th anniversary of diplomatic relations between Romania and the People's Republic of China. The 2013 Joint Declaration of the Governments of Romania and China on Deepening Bilateral Cooperation in New Circumstances, the Belt and Road Initiative (BRI) and the 14+1 Cooperation Format (the collaboration between China and Central and Eastern European countries - CEEC - focused on infrastructure, trade and cultural exchanges) acknowledge the economic, historical and cultural ties between the two countries. In July 2024, a memorandum of cooperation between the Chamber of Commerce and Industry of Romania and the China Council for the Promotion of International Trade (CCPIT) was signed at the The Romania-China Economic Forum (Sgueglia 2025).

Over the years, delegations of the Chinese People's Association for Friendship with Foreign Countries (CPAFFC) have met with high-ranking Romanian officials from the Ministry of Economy, the Ministry of Foreign Affairs, local officials and public institutions, with cultural or economic agendas. In terms of media cooperation, there are three main sources of Chinese information in Romania, in Romanian and English: China Radio International Romania (CRI Romania), the state-owned Xinhua news agency and the Chinese Embassy in Bucharest (Expert Forum 2022). Out of the 500 Confucius Institutes present in 190 countries, in Romania there are institutes in Bucharest, Cluj-Napoca, Brașov and Sibiu (Institutul Confucius 2025). Former chairman of the Defense, Public Order and National Security Committee, PNL deputy Pavel Popescu, has submitted a bill to the Romanian Parliament to block access to state budget funds for scientific research by Romanian universities collaborating with Confucius Institutes, accused of espionage for the Chinese Communist Party (Roman 2022).

Bilateral economic relations in the fields of infrastructure, technology and energy have led to renewable energy projects (solar power plants), collaboration on nuclear power plants at Cernavodă (collaboration with the Chinese company China General Nuclear Power Corporation – CGNPC – started in 2015, was suspended in 2020 following US recommendations; the US Justice Department accused CGNPC and Energy Technology International of nuclear espionage in April 2016 (Necșuțu 2020)) and conventional power plants at Turceni-Rovinari and Tarnița. China has also been involved in Romania's telecommunications infrastructure through the companies Huawei and ZT (Telekom). Romania later rejected Huawei's authorization for 5G equipment (Bicheno 2024), under the influence of Western countries' concerns about Huawei that led to the Prague Proposal on 5G infrastructure in 2019-2020, signed by 30 NATO and EU member countries (Benea 2024a). The 2017 law of the Communist Party of China, which requires Chinese companies to respond positively to requests for collaboration from Chinese intelligence agencies, as well as the arrest of a company employee for espionage, have fueled reluctance towards Huawei (Benea 2024a).

As of March 2024, China had registered over 13,697 companies in Romania, operating in the telecommunications, manufacturing, renewable energy and automotive sectors. Factories established in Brașov by Chinese companies NBHX and Ningbo Joyson Electronic Corp have created thousands of jobs in the automotive sector. The largest solar power plant in Romania is being developed by Chinese companies Intec Energy Solutions and Chint Group. The intermodal rail-sea transport to reach Constanța used by China Railway Express (Wuhan) connects and facilitates trade between China and Romania and the EU. The Green House program by the Romanian Government to subsidize solar panels in the households of Romanian citizens used components from Chinese manufacturers. By August 2024, trade between China and Romania increased by 26.4% compared to 2023, with China ranked 20th as the largest investor in Romania (Sgueglia 2025).

4.2. Hikvison and Dahua Under the Radar

Challenges for the China-Romania relations reside in the implementation of stricter foreign investment screening, which could hinder Chinese projects, in geopolitical factors, in Romania's

alignment with EU standards that could influence investment flows and in Chinese espionage and cyber attacks.

The RFE/RL (Radio Free Europe/Radio Liberty) investigation revealed that Hikvision and Dahua surveillance equipment, created by Chinese companies partially owned by the state, is used in at least 28 military units in Romania; also, the military base at Deveselu, where the NATO Aegis Ashore land-based missile defense system is operated together with the US military, uses Hikvision surveillance cameras, along with the coast guard and sites operated by the Romanian Intelligence Service (Standish 2024), Senate, prefectures, gendarmerie, police and customs (Mihai 2024), General Inspectorate for Emergency Situations, courts, city halls and universities in Romania (Benea Standish 2024).

Although the two companies have been banned in the US, UK and Australia over suspicions of possible links to the Chinese military, data storage methods and vulnerability to hacking, the Romanian Ministry of Defense says the use of cameras is legal and secure, as they are disconnected from the internet. Conor Healy, a surveillance industry expert at IPVM, believes that Hikvision and Dahua equipment can be hacked, even when not connected to the internet (Standish 2024). Although Hikvision has said there have been no security threats to its products, Marian Ghenescu, a video systems specialist, claims that these cameras can have both unintentional and intentional vulnerabilities. (Mihai 2024)

The Lithuanian Ministry of Defense discovered nearly 100 Hikvision vulnerabilities in 2021 that could expose it to malicious code injection or cyberattacks. No direct cybersecurity vulnerabilities were found at Dahua, but the company's cameras were shown to periodically send packets to servers in five countries, including China. Jens Stoltenberg, former NATO Secretary General, spoke out against the use of Chinese technology in critical infrastructure in September 2023 (Benea Standish 2024).

National security and sensitive information are at risk as firmware vulnerabilities could allow camera control, remote access, network attacks, and data interception by hostile governments, organized crime groups, and non-state actors. An FBI report from January 2024 shows how cameras disconnected from the internet can be accessed. The Chinese-backed hacking group *Volt Typhoon*, which targeted critical infrastructure, managed to hack a computer's operating system and then gain access to closed-circuit camera systems. Hikvision has been placed on a sanctions list in the US due to security concerns and human rights violations through the development of surveillance and tracking technology for Uyghurs and other minorities in the Chinese province of Xinjiang (Benea Standish 2024).

4.3. Romanian Members of Parliament under Chinese (Cyber) Attacks

The Chinese government follows *the Policy of Peaceful Reunification with Taiwan* without considering giving up, if necessary, the use of force. The Chinese commitment to *One country, two systems* requests the same point of view from other countries. In 2012, China thanked Romania for its support regarding Taiwan and Tibet, when the Romanian Delegation in China, led by the Romanian Secretary of State for Defense Policy Ion Mircea Plangu, was received by Chi Haotian, Minister of Defense, Vice Chairman of the Central Military Commission and State Counselor. Chi Haotian declared that the Chinese People's Liberation Army (PLA) is willing to strengthen the existing ties between the two armies. Plangu admitted the long-standing friendship between Romania and China and his belief that the mutual support will continue in the future (People's Daily Online 2012).

The relation between Taiwan and Romania is a current case study in the geopolitical context involving the European Union and China. The participation of Romanian MP Cătălin Teniță at the end of July 2024 at the fourth annual IPAC summit held in Taiwan, provoked a prompt reaction from China. While Beijing tried to discourage the participation of several IPAC members at the summit, the Chinese Embassy in Romania requested measures to control the behavior of certain members in relation to Taiwan in a letter sent to the headquarters of REPER, Cătălin Teniță's political party (Leonte 2024).

The Romanian political party REPER publicly responded to the Chinese Embassy that as long as the actions of its members comply with party rules and the law, it does not impose control over its members. The party aligns itself with the EU position of recognizing the One China policy, but also with

the European Parliament Resolution on the situation in the Taiwan Strait of September 2022, sharing with Taiwan common values such as the rule of law, democracy and human rights. In his public response to the letter, MP Cătălin Teniță also stated that, as an elected representative, he intends to explore opportunities for collaboration in sustainable urban development and in public services provision with the Taiwanese authorities. Although MP Cătălin Teniță visited Taipei in 2023, meeting with former President Tsai Ing-wen, the Chinese Embassy did not react. The political significance and visibility of the IPAC summit in Taiwan in 2024 probably contributed to China taking a position (Leonte 2024).

Some Romanian members of Parliament (MPs) wanted stricter rules on the use of Chinese technology in Romanian institutions of national security importance and sought to amend the legislation in parliament. For their critical attitude towards the Chinese government, three Romanian MPs, Alexandru Muraru (PNL), Cătălin Teniță (REPER) and former MP Pavel Popescu (PNL) were victims of espionage by APT31, a hacker group formed against *IPAC (Inter-Parliamentary Alliance for China)*, made up of parliamentarians from several countries who have accused the communist regime in China of human rights violations (Benea 2024b).

IPAC was established in 2020 to develop a strategy for democratic states to engage with China. In January 2021, hackers sent over 1,000 emails to over 400 accounts associated with IPAC. Those who opened the emails provided data about their location, the IP addresses of their devices and the type of browsers or operating systems used. The hackers also targeted institutions, politicians, businessmen and companies in the US and 43 MPs in the UK, not just IPAC officials within the EU. The FBI's investigation began in 2010, with a reward of $10 million for information leading to the capture of the seven men of Chinese origin (Benea 2024b).

Romania, like most EU countries, officially adheres to *the One China Policy*, with even more restrictive treatment of Taiwan than other European nations (Hungary has had a Taipei representative office in Budapest since the 1990s, a kind of de facto, not de jure, embassy of Taiwan). Romania hosts only a *TAITRA (Taiwan External Trade Development Council) Economic Office*, a non-profit organization that promotes trade between Taiwan and other countries. The Romanian Ministry of Foreign Affairs declared the lack of any official or inter-institutional relations with Taiwan. Romania prioritizes its political alignment and engagement with NATO, EU and USA, while restraining from provoking China (Leonte 2024).

Conclusions

The PRC poses a sophisticated and persistent cyber-espionage and attack threat to military and critical infrastructure systems, seeking to create destructive effects − from denial-of-service attacks to physical attacks on critical infrastructure in order to shape decision-making and disrupt military operations from the initial stages and throughout the course of a conflict.

Research becomes increasingly difficult as Western scholars will have to discern whether the people who can provide them with information or the sites they access are of good faith or want to disinform or recruit them. Like an acrobat, the Western researcher will be forced to resolve the tension between freedom of knowledge and his own security.

We appeal to the consideration encapsulated in the book *Power and Interdependence* by Robert Keohane and Joseph S. Nye, according to which the world is described by a complex interdependence (Keohane and Nye 1997). Our opinion goes in line with the two authors, because, as in the *chaos theory*, the flapping of a butterfly's wings in China risks triggering a tornado in Europe or America. The butterfly effect proves that the slightest change in the initial conditions leads to completely different results. States are not closed systems, they are in a continuous interaction, hence we need to pay attention and react properly to every change, to every new direction and especially to the tricky state of *status quo*, which is never everlasting, but tends to bend in one way or another. The Trio between China, USA and Russia always permitted during the decades the shift between the China-Russia friendship – the Treaty of Friendship, Alliance, and Mutual Assistance entered into

force on April 11, 1950 – to China-America friendlier relations during the Nixon Administration. The USA-Russia defrozen relations at the end of the Cold War were followed by the New Cold War between them, with China being on the Russian side and especially on its own side. The relational changes between the three powers affect the entire globe, and mostly the smaller countries.

Consequently, Romania must demonstrate great ability to take advantage of the economic and technological opportunities of the Asian area, while remaining loyal to Euro-Atlantic commitments. Also, it is desirable that young Romanians who have studied in China be attracted to work in and for Romania, their knowledge in Chinese culture and mentality contributing to the preservation of bilateral relations.

Spying is at the same time an ally and foe activity. Cyber intrusions could be considered interest coming from friends and too much attention coming from adversaries. Countries are interconnected, *no country is an island, so friendly or adversarial countries spying happens on a daily basis*, but when cyber security is at stake, its preservation is decisive for the countries' development and survival.

BIBLIOGRAPHY:

Baughman, Josh. 2024 "The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield. The Cyber Defense Review, Fall 2024, https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/Baughman_CDRV9N3-Fall-2024.pdf

Benea, Ionuț. 2024. "Ce înseamnă și de ce Bucureștiul a decis abia acum interzicerea Huawei în rețelele 5G din România". Europa Liberă România. 02 March, 2024. https://romania.europalibera.org/a/huawei-5g-romania/32844090.html

Benea, Ionuț. 2024. "Exclusiv | Parlamentari români vizați de o grupare globală de spionaj a Chinei. Cum au ajuns trei deputați ținte APT31". Europa Liberă România. 26 March, 2024. https://romania.europalibera.org/a/parlamentari-romani-spiotani-china/32878322.html

Benea Ionut, Reid Standish. 2024. "Chinese-Made Surveillance Cameras at Romanian Military Sites Raise Security Concerns". Radio Free Europe Radio Liberty. March 07, 2024, 21:43. https://www.rferl.org/a/romania-china-cameras-security-concerns/32853039.html

Bergengruen, Vera. 2022."How Ukraine Is Crowdsourcing Digital Evidence of War Crimes", The Time, April 18, 2022 6:00 AM EDT, https://time.com/6166781/ukraine-crowdsourcing-war-crimes/

Bicheno, Scott. 2024. "Romania rejects Huawei appeal against 5G ban". Telecoms.com. March 4, 2024. https://www.telecoms.com/5g-6g/romania-rejects-huawei-appeal-against-5g-ban

Chen, Zhuo. 2024. "Chinese PLA embraces a new system of services and arms: Defense spokesperson." China Military Online, 2024-04-19. http://eng.chinamil.com.cn/CHINA_209163/TopStories_209189/16302105.html

Expert Forum. 2022. "China's presence in Romania: The hundred flowers that never bloomed." China Watch. 7 October 2022. https://expertforum.ro/en/china-presence-in-romania/

Faligot, Roger. 2019. Serviciile secrete chineze de la Mao la Xi Jinping. Bucharest. Meteor Publishing.

Faligot, Roger. 2019. Chinese Spies. From Chairman Mao to Xi Jinping. United Kingdom C. Hurst & Co. (Publishers) Ltd.

Institutul Confucius. 2025. Universitatea Babes-Bolyai. https://confucius.institute.ubbcluj.ro/despre-noi/istoric_confucius/

Kania, Elsa B., John K. Costello. 2018. "The Strategic Support Force and the Future of Chinese Information Operations." Cyber Defense Review, Spring. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf

Keohane, Robert O., Nye, Joseph S. *Power and interdependence*. 1997.

Leonte, Andreea. 2024. "Romania's Strategic Puzzle: Navigating Taiwan Relations Amid Chinese Pressure". China Observers. 13 August 2024. https://chinaobservers.eu/romanias-strategic-puzzle-navigating-taiwan-relations-amid-chinese-pressure/

Lo Tien-Pin, Jason Pan. 2015. "PLA cyberunit targeting Taiwan named CYBERWAR SCHOOL? MND and MIB sources say the PLA's General Staff Department's Third Department has units in the guise of research centers and telecommunication labs. Taiwan News. Tue, March 10, 2015. https://www.taipeitimes.com/News/taiwan/archives/2015/03/10/2003613206

Mihai, Cătălina. 2024. "Romanian Army uses Chinese surveillance systems". EURACTIV.ro. February 20, 2024, 07:03. https://www.euractiv.com/section/politics/news/romanian-army-uses-chinese-surveillance-systems/?fbclid=IwY2xjawI8TodleHRuA2FlbQIxMAABHUUHnkSYfw8ZKJOX3L10kkORrHbTi1lS2mOHIjSzuubgnar7vhHdUzFxFA_aem_hDOxU51SuV4rXDQ4qUD0qw

Necsutu, Madalin. 2020. "Romania Cancels Deal With China to Build Nuclear Reactors". Balkan Insight. Bucharest. May 27, 2020. https://balkaninsight.com/2020/05/27/romania-cancels-deal-with-china-to-build-nuclear-reactors/

Office of the Secretary of Defense. 2023. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China. https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF

People's Daily Online. "Defense Minister Meets Romanian Delegation". http://www.peopledaily.com.cn/english/http://en.people.cn/english/200007/26/print20000726_46484.html?fbclid=IwY2xjawI8TsFleHRuA2FlbQIxMAABHWjl-BOM9QYtAqrlqugyqJNerNTfrrKBWZHJCloRH7lfKLOgwVxz-qA6XA_aem_lq7JWFRXAJBqCKxlwj7shg

Roman, Mihai. 2022. "Universitățile din România care colaborează cu Institutele Confucius din China vor pierde finanțarea pentru cercetare – proiect de lege". G4 Media, 24 November 2022. https://www.g4media.ro/universitatile-din-romania-care-colaboreaza-cu-institutele-confucius-din-china-vor-pierde-finantarea-pentru-cercetare-proiect-de-lege.html 24 Noi 2022.

Sgueglia, Giorgia. 2025. "China-Romania Economic Ties and 2025 Outlook." *China Briefing*. January 24, 2025. https://www.china-briefing.com/news/china-romania-economic-ties-and-2025-outlook/

Sharma, Deepak. 2010. "Integrated Network Electronic Warfare: China's New Concept of Information Warfare" (PDF). Journal of Defense Studies. April 4 (2): 37–38, https://idsa.in/system/files/jds_4_2_dsharma.pdf.

Shi, Zhan 2024. "The First Metaverse War". Reading the China Dream. September 15, 2024. https://www.readingthechinadream.com/shi-zhan-the-first-metaverse-war.html

Standish, Reid. 2024. "China In Eurasia Briefing: Chinese-Made Surveillance Equipment Used At Romanian Military Sites". Radio Free Europe Radio Liberty. March 13, 2024 11:38. https://www.rferl.org/a/china-romania-surveillance-technology-security-concerns/32859794.html?fbclid=IwY2xjawI8TvlleHRuA2FlbQIxMAABHWjl-BOM9QYtAqrlqugyqJNerNTfrrKBWZHJCloRH7lfKLOgwVxz-qA6XA_aem_lq7JWFRXAJBqCKxlwj7shg

Stokes, Mark A.. 1999. "CHINA'S QUEST FOR INFORMATION DOMINANCE." CHINA'S STRATEGIC MODERNIZATION: IMPLICATIONS FOR THE UNITED STATES. Strategic Studies Institute, US Army War College, 1999.

The Economist. 2023. "America and China try to move past a new bump in relations." 9th of June 2023. https://www.economist.com/china/2023/06/09/america-and-china-try-to-move-past-a-new-bump-in-relations

The Wall Street Journal. 2014. "Meet 3PLA, China's Version of the NSA." July 8, 2014, 3:45 am, https://www.wsj.com/articles/BL-CJB-23046