

TAIWAN (ROC) MUST ROCK! WHY TAIWAN'S CASE MATTERS?

*Malwina Ewa KOŁODZIEJCZAK; PhD**

Abstract: *The author discusses the subjectivity of Taiwan in the article. It must be remember that Taiwan is unrecognized as a state according to international public law. First then, author describes the theories of state elements. She also briefly characterizes the division of power in Taiwan. Then, she points to the organization of the cybersecurity system and methods of combating disinformation as an example of the efficient functioning of Taiwan as a state.*

Keywords: *Taiwan; unrecognized state; international public law; cybersecurity.*

Although Taiwan's international legal situation is complicated, Taiwan has experience in fighting disinformation and cognitive warfare, as well as potential that could be used by other states.

The main problem of the paper is contained in the question: What impact (if any) does Taiwan, as an unrecognized state, have on international law and security?

Therefore, the hypothesis comes down to the assumption that in international public law there are provisions whose interpretation allows for recognition, but there are no direct and explicit regulations. However, due to customary practice, the multitude of interpretations can bring different solutions. Thus, the lack of such clarity of law in this regard is unfavorable for both unrecognized states and the international environment.

The author will try to briefly present the most important legal regulations, problems with the recognition of Taiwan and the most important aspects contributing to Taiwan's security, as well as current security threats.

1. Taiwan according to International Public Law

According to Jellinek definition of the state must simultaneously consist of three elements: power, territory, population. Therefore, one of the most important criteria should be the stability and effectiveness of power over the territory and population and the capacity to enter into relations with other states. Increasingly, the ability to provide security and defense of the territory is added. Therefore, it is not international law that creates states, but states create international law. Nowadays, the state can be formed by secession, the dissolution of another state, the separation of territory from another state, or by merger/reunification of territories or, in fact, not currently practiced by the creation of a state in the territory of *res nullius*. A geopolitical unit, at the moment of acquiring legal capacity and capacity for legal action, becomes an entity according to public international law and can be recognized.

Lech Antonowicz said that: recognition of the states is one of the most complex and controversial institutions of international law. International practice in this area is uneven and scientific opinions are completely divergent. He believes that the recognition of newly created states is compulsory, provided that the criteria resulting from the definition of the state are met. That is why the topic of recognition of the R.O.C is extremely important both from the perspective of international public law and security.

The history of Taiwan is complicated and has a bearing on the current status of the island and the very use of the name Republic of China. The island - historically called Formosa, was under the protectorate of China, and even earlier of Japan. Following the adoption of the Cairo Declaration in 1943, which was incorporated into the Potsdam Proclamation of 1945, Taiwan was returned to Chinese administration¹. At the end of 1949, the Chinese Communist Party under Mao

* Doctor in security studies and currently is PhD candidate in law, War Studies University, Warsaw, Poland; e-mail: malwina.ewa.kolodziejczak@gmail.com.

¹ L. Antonowicz, *Status prawnomiędzynarodowy Republiki Chińskiej na Tajwanie*, [in:] *Tajwan w stosunkach międzynarodowych*, ed. by E. Halizak, Warsaw 1997, p. 38.

Zedong came to power in mainland China and proclaimed the People's Republic of China in Beijing. As a result of these events, the former authorities – the Kuomintang (KMT) and Chang Kai-shek² – moved to the island and in 1949 announced that the Republic of China in Taiwan was the one and only “China”, and the KMT was the only legal government, to which the People's Republic of China did not claim no rights. This situation was possible thanks to the support provided to the authorities in Taipei by the United States, which was accompanied by the "Sino-U.S. Agreement on Mutual Defense and Assistance" and the "Sino-U.S. Treaty on Mutual Assistance." What is important, at that time, Taiwan - as the Republic of China - was a member of the UN and also sat on the Security Council (!). Only in 1971 was Taiwan replaced by representatives of the government of the People's Republic of China.

However, in 1979 it was replaced by the "Taiwan Relations Act". It was only in the early 1990s that official talks began between Taiwan and the People's Republic of China. The President of the People's Republic of China, Chiang Tse-min, referring to Teng Hsiao-ping's concept of peaceful unification and "one country with two systems"³ from the 1970s, presented a cooperation proposal. This proposal received a response from Li Tenga-huej, who did not definitively reject the concept of unification. The effects of the lack of a clear refusal to this type of proposal are felt in relations between mainland China and Taiwan to this day.

The Constitution of Taiwan states that the Republic of China is based on "three political principles", i.e. a democratic people's republic, ruled by the people and for the people⁴. These are principles based on Sun Yat-sen's concepts. He also developed the concept of the "five powers", adding examination and control powers to the traditional tripartite division of state powers.

Contrary to the Montesquieu principle of separation of powers, popular in Western countries, a different division is in force in Taiwan. Power is divided between the juanas (transl. chambers/councils). According to the Constitution, there are: Executive Juan, Legislative Juan, Judicial Juan, Control Juan and Examining Juan. The equivalent of the government is the Executive Juan and the parliament is the Legislative Juan. The superior state body, which has the power to appoint people to many positions and mediate in disputes between the authorities, is the President.

It can be indicated that there are currently three prevailing concepts of the further political direction in which Taiwan should be heading: closer cooperation with mainland China (in the extreme case, unification), increasing independence until independence, and maintaining its current status.

Over the past few years, decision-makers and politicians in Taiwan have been trying to implement reforms and ensure economic and social development. It should be remembered that the country stabilized and began to implement the principles of a democratic state only in the early 1990s. Basically, enormous progress has been made, which is visible, for example, in the indicators of economic and innovative progress⁵. One of the biggest problems in the 1990s was the high rate of corruption among politicians, officials and judges. Currently, the corruption perception index surveyed by Transparency International placed Taiwan in 31st place among 180 assessed countries based on data for 2018⁶.

² Former power elites, party and government institutions of the National Party – Kuomintang (KMT) and the command of the destroyed army, along with their families, evacuated to the island (approximately 1.6 million people in total), taking away national treasures, museum collections, some archives, and the achievements of the Academy of Sciences (Academia Sinica) and other "national institutions and symbols", and in Taipei, next to the authorities of Taiwan Province, the central authorities of the Republic of China began to function, headed by the parliament elected in 1947 and the president. The Constitution of 1946 and the ideology of Sun Yat-sen's "three principles of the people" were also in force, on whose concepts the state system and the KMT ideology were based. These principles are translated, in principle, which in principle are translated as: "nationalism" (minzuzhui) – more as "state patriotism", democracy (minquanzhuyi) and "people's well-being" (minshengzhuyi). Vide: K. Gawlikowski, *Tajwan: spory o status wyspy i procesy transformacji*, [in:] *Azja Wschodnia na przełomie XXI XXI wieku: przemiany polityczne i społeczne*, ed. by K. Gawlikowski, M. Ławacz, Warsaw 2004, pp. 165-236.

³ This concept was later implemented in relations between China, Hong Kong and Macao.

⁴ *Constitution of the Republic of China 1947*, art. 1.

⁵ Vide: *Profil terytorialny Tajwanu*, <https://poland.tw/resource/0bee84ac-aaca-44f6-b6fe-20b3ed9f1114:JCR> [10.06.2024].

⁶ <https://www.transparency.org/country/TWM> [09.06.2024].

2. Cybersecurity as an example of the most important element of the national security

Cybersecurity in Taiwan has been playing a key role in the country's defense for several years and is perceived on an equal footing with national security. This should not be surprising, given Taiwan's problematic international legal status. For this reason, Taiwan is trying to strengthen its position in cyberspace and develop cybernetic capabilities – improving not only legal regulations, system organization, but also technological properties.

The reason why cybersecurity considerations are so important for Taiwan is the numerous attempted hacker attacks carried out from outside, including: through other international entities. These issues should be combined with the elements of disinformation or even the so-called "information war". Moreover, it is often pointed out that cyber attacks, but also fake news, infected applications, etc. are a common element of this practice. Therefore, cybersecurity is of particular importance in Taiwan and is also considered in the context of military security.

For this reason, cybersecurity in various dimensions – both legal and organizational – is becoming increasingly important in the government's policy, strategy and activities. The new Cybersecurity Management Act⁷, together with six implementing acts⁸, creates complete regulations in this area.

The purpose of the act was to implement the national information security policy and build a secure IT environment to protect national security and the well-being of society. The Act also defines the IT system, information security, information security incident and critical infrastructure.

In addition to passing the Cybersecurity Management Law and establishing a special cybersecurity cell – DCS – in the Executive Yuan, the government created or remodeled agencies, developed training programs and developed cooperation with the private sector to strengthen the cybersecurity system. The current cybersecurity system in Taiwan has been transformed into an "iron triad" consisting of⁹:

- National Information and Communications Security Office (NICSO) operating under the National Security Council (NSC);
- Department of Cyber Security (DCS) with a separate National Information and Communication Security Taskforce (NICST) operating under the Executive Yuan;
- National Communications and Cyber Security Center (NCCSC) under the National Communications Commission (NCC).

NICSO reports directly to the President, while DCS reports to the Prime Minister. The above-mentioned institutions and bodies, together with separate units of the Ministry of Interior (MOI), Ministry of National Defense (MOND), Ministry of Science and Technology (MOST) and Ministry of Economy (MOEA), create Taiwan's cybersecurity system.

In turn, the National Information and Communication Security Taskforce (NICST) was created in January 2001 by Executive Juan. Its tasks are managed by DCS. NICST is responsible for developing national cybersecurity policy, establishing reporting and response mechanisms, promoting interagency coordination, and overseeing cybersecurity matters.

It should be mentioned that there are three main institutional entities in Taiwan's cyber defense infrastructure: the National Security Bureau, the Ministry of National Defense and the

⁷ *Cybersecurity Management Law 2018*, vide: <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297> [16.06.2024].

⁸ *Regulations on the Notification and Response of Cyber Security Incident, Regulations on Classification of Cyber Security Responsibility Levels, Regulations on Audit of Implementation of Cyber Security Maintenance Plan of Specific Non-Government Agency, Regulations of Special Non-official Agencies' Cyber Security Management by National Communications Commission, Enforcement Rules of Cyber Security Management Act, Cyber Security Information Sharing Regulations*, vide: <https://law.moj.gov.tw/ENG/Law/LawSearchResult.aspx?ty=ONEBAR&kw=cyber> [16.06.2024].

⁹ Bo-Jiun Jing, *Cybersecurity as a Sine Qua Non of Digital Economy: Turning Taiwan into a Reliable Digital Nation?*, [w:] *Taiwan Security Brief: Disinformation, Cybersecurity, & Energy Challenges*, ed. by Y. Tatsumi, P. Kennedy, J. Li, Stimson, 2019, p. 29.

Criminal Investigation Bureau. Civilian and military institutions have developed common operational and protective mechanisms, and use various exercises and training to materialize the concept of critical infrastructure protection in the context of cyber threats in order to improve and strengthen information security protective capabilities¹⁰. For this purpose, the Information Communication Electronic Force Command (ICEF) was created three years ago, de facto the fourth branch of the armed forces¹¹.

The above outline of the cybersecurity system indicates that Taiwan is constantly strengthening its cyber capabilities, not only in the field of cyber defense, but also in the broadly understood development of the digital economy, to which cyber security is key.

3. Disinformation as an example of the most important threat

Disinformation, not only from the Chinese-Taiwanese perspective, is related to propaganda activities and information warfare elements with the use of mass media. Current information warfare mechanisms allow effective operations aimed at directing the adversary's decision-making patterns. Information entered to the state, but hidden, as well as data patterns of a specific country (including false information) should affect the society and evoke reactions consistent with the manipulator's intentions¹².

The new National Cyber Security Program of Taiwan 2021-2024 lists 6 potentially most probable types of threats related to attacks in the cyberspace: "the intensification of personal data and digital certification leakage attacks", "the proliferation of ransomware attack risks", "the increase of threats of vulnerabilities of IoT and mobile devices", "APT targeted attacks to steal confidential data", "the hacking of cyber security (information) suppliers destroying supply chain security" and "the multiplication of critical information infrastructure security risks"¹³. These threats might occur parallel to the elements of Chinese propaganda, including the dissemination of false information related to actual facts, or vice versa, which is currently a widespread phenomenon.

Moreover, the People's Republic of China has been using modern propaganda measures for several years now. According to Chinese doctrine, cognitive warfare is unlimited in time and space, it is targeted, and affects the mentality and will of adversaries. It expands on the PRC's "Three Warfares" and united front tactics, stressing that propaganda must transgress "into the island (Taiwan), every household, everyone's head, and ultimately individual's mind". These activities are combined with hacker attacks and disinformation, and are aimed at attempting to influence public opinion, manipulating the evaluation of public authorities' operations, and sometimes creating panic, fear, and suspicions among the society, so as to ultimately destroy their trust in the Taiwanese government. Currently, social media are mostly used to spread disinformation that is produced fast and on a mass scale, but is meticulously prepared. To counteract the cognitive warfare tactics of the PRC, the Armed Forces of ROC established mechanisms for fast response in the society and fostered education in this sphere. In the meantime, strategic communication activities were also carried out to provide explanations on time and earn the understanding and support of the international community¹⁴.

¹⁰ Li-Chung Yuan, *The Role of Military in Cyberspace: Case of Republic of China (Taiwan)*, [w:] *Securing Cyberspace. International And Asian Perspectives*, ed. Ch. Samuel, M. Sharma, Institute for Defence Studies & Analyses New Delhi, Pentagon Press, 2016, s. 290-291.

¹¹ S. Yeh, E. Hou, *Information, communication and electronic warfare command formed „Focus Taiwan”* (27.06.2017), vide: <https://focustaiwan.tw/politics/201706290027> [15.06.2024].

¹² R. Bielawski, B. Grenda, *Wybrane zagadnienia cyberbezpieczeństwa narodowego*, Wrocław 2019.

¹³ National Information and Communication Security Taskforce, Executive Yuan, *National Cyber Security Program of Taiwan (2021 to 2024) Republic of China (Taiwan)*, 2021.

¹⁴ *Quadrennial Defense Review Republic of China, 2021*.

4. Conclusion

Taiwan knows well, “as the old saying goes, it is a bad idea to bring a knife to a gun fight; so too it is a bad idea to use a conventionally armed, equipped, trained, and organized military force as the principle means to fight what is primarily an informational war - a war that requires a more nuanced sophisticated, flexible, and distributed approach”¹⁵.

Although Taiwan has made significant progress in cybersecurity, it still faces challenges in this area due to increased attempts and attacks. As indicated in reports and analyses, the main challenge is integration and cooperation between countries and continuous improvement of the cybersecurity system and infrastructure. Cooperation with other countries is therefore necessary, and areas of cooperation could include the protection of critical infrastructure, including telecommunications networks, financial systems and electricity supplies, and the adaptation of regulations to international regulations on cyber issues. Therefore, cooperation with the United States and European states seems invaluable Taiwan has potential in this field and, due to its geopolitical location and Taiwan's experience with attacks from Chinese organizations, other states could also derive tangible benefits from mutual relations in the field of cybersecurity.

Disinformation activities deployed in Taiwan, including fake news, are aimed at interference in democracy. However, it should be stressed that disinformation campaigns in Taiwan are producing increasingly weak results. This is owing to system-based and legal and organisational measures. The approach of the authorities, conveying accurate and clear information and implementing a transparent health policy, is vital here. Another greatly important element is education in the sphere of combating fake news and improving resilience to disinformation campaigns, with activities addressed both to children and the older population.

¹⁵ D.A. Borer, *Why is information strategy difficult?*, [w:] *Information Strategy and Warfare. A guide to theory and practice*, red. J. Arquilla, D.A. Borer, p. 236.

BIBLIOGRAPHY

1. *Constitution of the Republic of China 1947*.
2. *Cybersecurity Management Law 2018*.
3. National Information and Communication Security Taskforce, Executive Yuan, *National Cyber Security Program of Taiwan (2021 to 2024) Republic of China (Taiwan)*, 2021.
4. *Quadrennial Defense Review Republic of China*, 2021.
5. Antonowicz L., *Status prawnomiędzynarodowy Republiki Chińskiej na Tajwanie*, [in:] *Tajwan w stosunkach międzynarodowych*, ed. by E. Halizak, Warsaw 1997.
6. *Azja Wschodnia na przełomie XX i XXI wieku: przemiany polityczne i społeczne*, ed. by K. Gawlikowski, M. Ławacz, Warsaw 2004.
7. Bielawski R., Grenda B., *Wybrane zagadnienia cyberbezpieczeństwa narodowego*, Wrocław 2019.
8. Bo-Jiun Jing, *Cybersecurity as a Sine Qua Non of Digital Economy: Turning Taiwan into a Reliable Digital Nation?*, [w:] *Taiwan Security Brief: Disinformation, Cybersecurity, & Energy Challenges*, ed. by Y. Tatsumi, P. Kennedy, J. Li, Stimson, 2019.
9. Borer D.A., *Why is information strategy difficult?*, [w:] *Information Strategy and Warfare. A guide to theory and practice*, red. J. Arquilla, D.A. Borer.
10. Li-Chung Yuan, *The Role of Military in Cyberspace: Case of Republic of China (Taiwan)*, [w:] *Securing Cyberspace. International and Asian Perspectives*, ed. Ch. Samuel, M. Sharma, Institute for Defence Studies&Analyses New Delhi, Pentagon Press, 2016.
11. <https://focustaiwan.tw/politics/201706290027> [15.06.2024].
12. <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297> [16.06.2024].
13. <https://poland.tw/resource/0bee84ac-aaca-44f6-b6fe-20b3ed9f1114:JCR> [10.06.2024].
14. <https://www.transparency.org/country/TWM> [09.06.2024].