Cybersecurity as an Instrument of State Power: Evaluating the Republic of China's (ROC's) Information, Communications, and Electronic Force Command (ICEFCOM) Against the People's Republic of China's (PRC's) Escalating Threats

Willis Wang

Was the Republic of China's (ROC's) decision to form a new cyber defense command due to an increasing number of cyberattacks from external threats, especially from the People's Republic of China (PRC)? This paper examines how increasing Chinese cybersecurity threats targeted at the ROC led to the establishment of ICEFCOM under President Tsai Ing-wen's administration. Specifically, this paper seeks to unravel whether the formation of ICEFCOM under President Tsai Ing-wen's administration was a direct response to various Chinese cybersecurity attacks, including Distributed Denial of Service (DDoS) attacks, SQL Injection, and Advanced Persistent Threat (APT) Groups. By scrutinizing the intricate dynamics of these cyber confrontations and the subsequent defensive measures taken by the ROC, this study endeavors to illuminate the pivotal role of ICEFCOM in bolstering its cybersecurity capacity. The paper concludes, with empirical analysis, that a correlation exists between the ROC's response to the Chinese cyber threats and the strategic formation of the ICEFCOM during President Tsai Ing-wen's tenure.

The ROC Ministry of Defense (MND) created its Information, Communications, and Electronic Force Command (ICEFCOM) in 2017 to meet growing cybersecurity challenges. ICEFCOM increases the ROC's multi-domain deterrence capacity against PRC cyberattacks. But was its formation specifically driven by the PRC's actions? This paper adopts two approaches to argue that the ROC decision to create the new command was a response to escalating cybersecurity attacks on the nation. This study examines the annual budgets within ICEFCOMs' three forces: Army Command Headquarters (HQ), Navy Command HQ, and Air Force Command HQ. The work then identifies whether annual ICEFCOM budget increases within the Army, the Navy, and the Air Force exist. The study elaborates on cyber-war exercises between ICEFCOM and other countries, primarily the U.S. and Japan. Doing so identifies examples of closer collaboration between the ROC's military cyber forces and those of other countries. A significant limitation of this approach is the superficial descriptions of ICEFCOM's activities in open-source literature.

Willis Wang graduated from Georgetown University in 2021 with a Bachelor of Science degree in International Politics and a certificate in Japanese. He previously published research papers with Cornell, Georgetown, and the London School of Economics. He currently serves as a supply chain analyst at the Peter Wang Trading Company.

This research topic merits more attention for several reasons. The PRC is an ongoing threat to the ROC's regime survival, as it has never renounced its use of force to take over the island.[1] According to the ROC's National Center for Cyber Security Technology, China launches twenty to forty million cyber-attacks per month against the ROC.[2] Cyber-war exercises among the ROC and other countries (primarily the U.S.) both strengthen the ROC's military and elevate its international status. Cybersecurity is a current concern to both the U.S. and the ROC. Through the U.S.-led Global Cooperation and Training Framework (GCTF), the U.S., Japan, and the ROC closely cooperate on joint cyber exercises.[3] Finally, better understanding the origins and mission of ICEFCOM could boost Taiwanese public morale.

What Factors Led to the Upgrade from the Three IEFCOMs to ICEFCOM?

This section discusses the increasing cyberattacks from the PRC towards the ROC, which led to the formation of ICEFCOM and elaborates on ICEFCOM's institutional structure. This structure informs military planners and readers about the budget, objectives, and future courses of action for the command.

The PRC's escalating cyberattacks on the ROC drove ROC's creation of ICEFCOM. China's military launched more than 30 million cyber-attacks per month towards the ROC from 2014 to 2020.[4] The Third Department, the home command of these attacks, is likely responsible for strategic level planning, including collecting signals intelligence (SIGINT) and planning in accordance with the PRC's Integrated Network and Electronic Warfare doctrine. Its Second Division presumably is responsible for tactical and operational levels of military actions, including Distributed Denial of Service (DDoS) attacks, SQL Injection, and Advanced Persistent Threat (APT) Groups.[5] Chinese cyber forces targeted the Taiwanese civilian social media accounts on Facebook, Instagram, and Line[6], and attacked some of the ROC's most critical military institutions, including the MND Main Webpage, the National Defense University, the MND's Recruiting Center of National Armed Forces, the MND Medical Affairs Bureau, and the MND's Political Warfare Bureau. In 2019 July, Chinese hackers stole at least 59,000 Taiwanese government officials' personal information, later selling some of it on the

---

[1] Lun-Tian Yew, "Attack on The Republic of China an Option to Stop Independence, Top China General Says," *Reuters,* May 28, 2020, https://www.reuters.com/article/us-china-The Republic of China-security/attack-on-The Republic of China-an-option-to-stop-independence-top-china-general-says-idUSKBN2350AD.

[2] Huang Tzu-ti, "The Republic of China Government Websites Hit with Over 20 million Cyber Attacks a Month, Mostly from China," *The Republic of China News*, April 5, 2018, https://www.The Republic of Chinanews.com.tw/en/news/3398654.

[3] Pei-ju Teng, "The Republic of China, U.S., and Japan Co-host Workshop on Cybersecurity," *The Republic of China News*, May 28, 2019, https://www.The Republic of Chinanews.com.tw/en/news/3712340.

[4] Aaron Tu, Chung Li-hua, and Jake Chung, "Tsai Swears in Cyberwar Commander," *Taipei Times*, June 30, 2017, http://www.taipeitimes.com/News/The Republic of China/archives/2017/06/30/2003673594. The article specifically identifies the Second Division of the Third Department of the People's Liberation Army General Staff Department, the People's Liberation Army Advanced Persistent Threat (APT) Unit with Military Unit Cover Designators (MUCDs) 61398, 61486, 61449, and 78020 Units, as the perpetrators of these attacks.

[5] In DDoS attacks, the aggressor intentionally overloads servers to jam a computer. SQL injections revolve around the use of malicious code and target a computer's MS SQL Server database. Phishing is the use of malicious emails that pretend to be a well-credited company to deceive the victims to click and access malicious links.

[6] Line is a popular social media application in Japan, Taiwan, Thailand, and Indonesia. "Why is LINE the most poplar social media app in Japan?", *Digital Marketing for Asia,* https://www.digitalmarketingforasia.com/why-line-is-the-most-popular-social-media-app-in-japan/.

dark web.[7] These cyberattacks continue to target the ROC's critical infrastructure.

ICEFCOM is designed specifically to equip the ROC with a stronger capacity to deter China's cyberattacks, even though it nominally has a different command structure than similar organizations. In peacetime, ICEFCOM integrates MND's network, electronics, and information communication platforms to ensure effective communication.[8] ICEFCOM also implements maintenance for cyberspace security and electromagnetic reconnaissance.[9] In wartime, ICEFCOM will assist the defense of the ROC's critical information infrastructure to secure the country's physical territory and cyber space. The MND does not label ICEFCOM as a military agency in the same way as the Army Command HQ (ROCA), Navy Command HQ (ROCN), and Air Force Command HQ (ROCAF). According to the MND's 2019 National Defense Report, ICEFCOM is coordinated with Reserve Command and Military Police Command.[10] In peacetime, the latter two specialize in defense and logistical aspects of national security. Therefore, the institutional alignment of this new organization appears partially aimed at not provoking the PRC.

The upgrade from individual service IEFCOMs to an integrated ICEFCOM is significant for integration and coordination purposes. Prior to the integrated ICEFCOM, the Communication Development Office of the General Staff Headquarters (MND-GSH-CDO) and the Information and Electronic Force Commands (IEFCOMs) in ROCA, ROCN, and ROCAF conducted Taiwanese cyber operations. However, the CDO and IEFCOMs in each military agency acted independently. This lack of coordination caused problems for interoperability within the cybersecurity capacity. The transition to a joint ICEFCOM solves the issue of strengthening inter-operability. ICEFCOM Chief of Staff Ting-Shen Li explained that, prior to the integration, the three IEFCOMs acted as "telecom maintenance units" that focus solely on their respective forces' independent headquarters, different telecommunications, various strategy development rooms, and, most problematically, distinct military culture.[11] Chief of Staff Li asserted that, after the integration, the ICEFCOM can work more closely on assigned tasks.

Is there a Relationship between Number of Cyber Attacks that the Republic of China Faces and Increases in ICEFCOM's Budget?

Moving from a qualitative assessment of Taiwanese intentions, this section explores the quantitative aspect of ICEFCOM's origins. There is no question that the number of Chinese cyber-attacks on the ROC are increasing. MND Spokesperson Colonel Yi-Chang Lin asserts that the ROC experienced approximately 204 million cyber-attacks in 2017; 299 million cyber-attacks in 2018; and 300 million cyber-attacks in 2019.[12] ROC Congresswoman Wu Yu-Chin

---

[7] Lin-Jun Xie, "59,000 data of officials from the Ministry of Civil Service Stolen", *Liberty Times Net*, July 14, 2019, https://news.ltn.com.tw/news/politics/breakingnews/2852408.

[8] Shieng-Shin Su, "Policy Analysis on the Construction of Information, Communications and Electronic Force Command," *Legislative-Yuan ROC,* November 2017, https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=176016#.

[9] Shieng-Shin Su, "Policy Analysis."

[10] "The 2019 National Defense Report," *Ministry of National Defense* of the *ROC*, 2019, https://www.usThe Republic of Chinadefense.com/tdnswp/wp-content/uploads/2020/02/The Republic of China-National-Defense-Report-2019.pdf.

[11] Yen-Xin Huan, For the First Time Ever, MND Discusses its Cyberwarriors," ITHOME Technology Magazine, July 7, 2017, https://www.ithome.com.tw/news/115460 .

[12] Ying-Yu Lin, "Strategic Importance on Information Warfare to the National Defense Operations," *Navy Command ROC*, October 2017, https://navy.mnd.gov.tw/Files/Paper/8-資訊戰對國軍防衛.pdf, page 123.

notes that, while the ROC intercepts 99.99% of cyber-attacks from foreign powers, the missing 0.01 percent usually result in serious damages like the previously mentioned leaks.[13]

The figures for ICEFCOM's budget from 2017 to 2021 offer a mixed signal. According to the 2017-2021 Fiscal Year (FY) Budget of the Ministry of National Defense, the ROCA ICEFCOM budget did not show an annual increase as predicted.[14] However, the overall trend for the ROCN and ROCAF ICEFCOM budgets is positive, showing an annual increase (excluding the FY2021 budget).[15] This observation seems to support the argument that the ROC is increasing its budget to defend its primary aggressor. In terms of ROCA, however, numbers show a mixed sign. While FY 2018 shows a decrease of 30 percent compared to FY2017, the year when ICEFCOM was founded, FY 2019 continued to show a decrease of approximately two percent compared to FY2018.[16] After the two decreases in consecutive years, FY 2020 shows an increase of nine percent compared to FY 2019. While the initial cost (FY2017) to create ICEFCOM in ROCA is understandable, a significant decrease of nearly 30% between FY2017 and FY2018 is puzzling. A numerical of these variances is provided below in Table 1.

Table 1: ICEFCOM's Service Budgets FY 2017-2021 (in 1000s of New Taiwanese Dollars (NTD))[17]

	FY2017	FY2018	FY2019	FY2020	FY2021 (pending)	Total (w/o FY2021)	Total (incl FY2021)
ROCA	672,667	467,805	458,578	502,971	469,020	2,102,021	2,571,041
ROCN	353,563	355,563	360,251	431,776	369,609	1,503,153	1,872,762
ROCAF	447,664	451,407	463,294	529,194	457,335	1,891,559	2,348,914

What factors explain the 30% decrease in ROCA ICEFCOM's FY 2017 and FY 2018 Budgets? One clue is in budget statements for "Military equipment and facilities": FY2017 shows a cost of 224,927 NTD while FY2018 stipulates an outlay of only 3877 NTD.[18] FY 2017 cryptically

[13] "The 1st Joint Meeting of the Finance, Justice and Legal Affairs Committee," *Legislative Yuan ROC*, October 28, 2020, https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=43988&pid=203529.

[14] "The 2017 Statutory Budget Statement of the Ministry of National Defense", https://www.mnd.gov.tw//NewUpload/201710/106年度國防部所屬單位法定預算書表_501068.PDF; "The 2018 Statutory Budget Statement of the Ministry of National Defense, https://www.mnd.gov.tw//NewUpload/201803/107年度國防部所屬單位法定預算書表_115897.PDF; "The 2019 Statutory Budget Statement of the Ministry of National Defense", https://www.mnd.gov.tw//NewUpload/201904/108年度國防部所屬單位預算書表_531330.PDF; "The 2020 Statutory Budget Statement of the Ministry of National Defense", https://www.mnd.gov.tw/NewUpload/202004/109年度國防部所屬單位法定預算書表%20_572871.pdf; "The 2021 Statutory Budget Statement of the Ministry of National Defense," https://www.mnd.gov.tw//NewUpload/202009/110年度國防部所屬單位預算案書表_274102.pdf. All documents published by Republic of China Ministry of National Defense, Taipei, The Republic of China.

[15] Statutory Budget Statements.

[16] Statutory Budget Statements.

[17] Created by Author, derived from Statutory Budget Statements.

[18] "2017 Statutory Budget Statement", 148; "2018 Statutory Budget Statement", 156.

refers to this expense as "Installation of network equipment of the Xun'an communication system software to implement the military equipment and facilities." While FY 2018 also included maintenance of the Xun'an communication system software, the cost is nowhere near that of FY 2017. It is reasonable to assume that ICEFCOM had purchased new (presumably classified) equipment or invested hugely in communication capacity in FY 2017.

Another explanatory factor is the "Maintenance of military equipment and facilities" category, where the FY2017 Report reflects a total of 330,705 NTD while the FY2018 shows a total of 323,012 NTD.[19] The FY2017 figure reflects MND installation and maintenance of communication and information wires, sea and ground cables, optical fiber, radio, and similar backbone infrastructure. FY2018 spending is categorized as maintenance of the Xun'an System, Tactical Area Communication System Software Support, and other equipment. The limited information available shows that ICEFCOM increased its communication capabilities to a certain extent beyond mere maintenance in FY2017.

Is There a Relationship Between Numbers of Cyber Attacks That the ROC Faces and Numbers of Joint Cyber-related Exercises that The ROC Conducts with Other Countries?

This section begins by looking at the number of cooperative cyber events ICEFCOM executes. While the data for this section is limited, as the MND does not provide detailed descriptions of the events, Table 2 provides a summary of those interactions. The MND engages primarily with the U.S. and other European countries in the "Link 16 System International Conference" and "International Multilateral Working Groups Conference." It is noteworthy that the listed events are solely ROCA and ROCAF; no information on ROCN events is available in open-source literature. It is therefore difficult to draw a correlation between increased Chinese cyber-attacks and increased Taiwanese military cyber cooperation with other countries.

[19] Please refer to page 105 of the 2017 Statutory Budget Statement and page 106 of the 2018 Statutory Budget Statement.

Table 2: Service ICEFCOM Events with Other Countries, FY 2017-2020[20]

Year	Event	Service	Country
FY2017	Project *Tactical Area Communication System* Software	ROCA	U.S.
	Annual Fair of the Association of Old Crows (AOC	ROCAF	U.S.
	Information and Electronic Force Operations Conference	ROCAF	U.S.
	Link 16 System International Conference	ROCAF	U.S.
FY2018	A Study Trip to the Georgia Military College	ROCA	Georgia, U.S.
	Information and Electronic Force Operations Conference	ROCAF	U.S.
	Link 16 System International Conference	ROCAF	U.S.
	Black Hat USA	ROCAF	U.S.
FY2019	A Study Trip to the Georgia Military College	ROCA	Georgia, U.S.
	Annual Fair of the Association of Old Crows (AOC	ROCAF	U.S.
	Information and Electronic Force Operations Conference	ROCAF	U.S.
	International Multilateral Working Groups Conference	ROCAF	European Countries
	Black Hat USA	ROCAF	U.S.
FY2020	A Study Trip to United States Indo-Pacific Command (INDOPACOM)	ROCA	U.S.
	International Multilateral Working Groups Conference	ROCAF	European Countries
	Black Hat USA	ROCAF	U.S.
	Annual Fair of the Association of Old Crows (AOC)	ROCAF	U.S.
	Information and Electronic Force Operations Conference	ROCAF	U.S.

It is possible to make two generalized observations about ICEFCOM cooperation with other countries. Both the ROCA and ROCAF ICEFCOM use military schools in the U.S. to establish closer ties with America. Because the U.S. prohibits Taiwanese personnel from wearing military uniforms in the U.S., ROCA/ROCAF members must interact with U.S. military personnel and soldiers as civilians.[21] ICEFCOM continues to join U.S.-led international civilian cyber events, such as the Association of Old Crows (AOC) and Black Hat, which also further ROC-U.S. cyber cooperation. While no specific data shows the exact activities that happened during these cybersecurity events, the ROC participation in them suggests a shared desire to counter Chinese cyber activity.

Two other events reflect the robust U.S.-ROC cooperation in cyber defense. To celebrate the 40th anniversary of U.S.-ROC relations in 2019, the American Institute in Taiwan (AIT) launched the first five-day U.S.-ROC Cyber Offensive and Defensive Exercise (CODE).[22]

---

[20] Created by Author, derived from Statutory Budget Statements FY 2017-FY 2020. No additional detail on which European Countries participated is available in source documents.

[21] "107th Congress First Session Committee Print: U.S. Defense Policy Toward The Republic of China: In Need of An Overhaul," *U.S. Government Publishing Office*, April 2001, https://www.govinfo.gov/content/pkg/CPRT-107SPRT71658/html/CPRT-107SPRT71658.htm#:~:text=However%2C%20the%20U.S.%20Government%20imposes,train%20in%20the%20United%20States..

[22] "The Republic of China and U.S. co-hosting multinational cybersecurity exercise," *Department of Information Services of the Executive Yuan*, November 6, 2019, https://english.ey.gov.tw/Page/61BF20C3E89B856/0f357b66-7ed3-4123-98c6-

According to the Vice Premier of the National Information and Communication Security Taskforce (NICST) Convener Chen Chi-Mai, the CODE exercises are similar to the U.S. CYBER STORM biannual cyber exercises conducted by the U.S. Department of Homeland Security. CODE exercises are rare opportunities for ROC to gain hands-on experience in cyber defense from the U.S. Another U.S.-ROC cooperative venue is the July 2020 U.S.-ROC Cybersecurity Forum on 17 July 2020 in Taipei co-hosted by the Ministry of Economic Affairs Department of International Cooperation and the AIT.[23] The experts from both sides discussed emerging cyber threats and technology to defend private firms and governments from these cyber-attacks. This event also shows a robust relationship between the ROC and the U.S.

Conclusion: Formation of the ICEFCOM and the Fundamental Differences on Cyberspace Between the PRC and the US-led International Order

This paper shows that the ROC's decision to increase its spending on ICEFCOM is a response to the escalating cybersecurity attacks caused by China. However, an examination of empirical data pertaining to ICEFCOM's budget in the ROC between 2017 and 2021 demonstrates a varied trajectory that reflects nuanced trends or fluctuations. The overall trend for the ICEFCOM budget in ROCN and ROCAF indicates a positive annual increase, except for the FY2021 budget, while the budget for ICEFCOM in ROCA did not increase annually as predicted. The budget for ROCA shows a mixed signal because the money does not necessarily indicate a positive slope year by year. A relatively high cost in Military Equipment and Facilities category is the most likely explanation for this outlier. The ROC continues to conduct cyber activities with the U.S. and other countries as well.

In the future, as cross-strait tension continues to escalate, ICEFCOM will continue to strengthen its interoperability with the U.S. military. Clear communication, mutual trust, and capacity will continue to be critical elements to defeat authoritarian adversaries. Moving forward, the ROC's collaboration with strategic allies and partners, notably the United States and other like-minded democratic countries, contributes to fostering the US-based international cybersecurity norms. As the digital realm continues to evolve as an instrument of state power, cross-border cooperation and technological prowess and the preservation of individual privacy remain strategically important.

b91097b82536. The American Institute in the ROC functions as a *de facto* U.S. Embassy, since the U.S. has no formal diplomatic relations with the ROC under the "One China" policy.

[23] "Cybersecurity forum staged by The Republic of China, U.S. in Taipei," *The Republic of China Today*, July 20, 2020, https://The Republic of Chinatoday.tw/news.php?unit=2,6,10,15,18&post=181583.