Trends and Prospects of the Eastward Expansion of NATO Cybersecurity Cooperation

Li Yan and Zhou Ningnan *

Abstract: With the evolving international situation, particularly the Ukraine crisis, NATO's strategic focus has accelerated its shift toward the Asia-Pacific and cyberspace. Asia-Pacific countries, such as India, Singapore, and Thailand, also seek to strengthen cooperation with NATO in cybersecurity. At the same time, the Ukraine crisis has played a catalytic role in accelerating the eastward expansion of NATO's cybersecurity mechanism. The eastward expansion of NATO's cybersecurity mechanism is an important means for NATO to implement cyber deterrence in the Asia-Pacific region, particularly the strategic containment of China. This has hurt the cybersecurity situation in the Asia-Pacific region and even the world, causing widespread concern in countries throughout the Asia-Pacific region about the deteriorating cybersecurity situation. Influenced by multiple factors, the eastward expansion of NATO's network security mechanism has clear momentum. In the long run, however, the strategic intention of NATO's eastward expansion does not fully align with the security needs of Asia-Pacific countries, resulting in uncertainty about further development in the future.

Keywords: NATO, cybersecurity cooperation, eastward expansion

In recent years, under the influence of multiple factors, including shifts in its strategic focus and the Ukraine crisis, NATO's cybersecurity mechanism has continued to expand eastward toward the Asia-Pacific region. The influence of NATO's cyber strategy on relevant Asia-Pacific countries has increased, and cybersecurity cooperation has been continuously consolidated.

* Li Yan is executive director and research professor at the Institute of Sci-Tech and Cyber Security at China Institutes of Contemporary International Relations (CICIR). Her research fields include strategies of science and technology and cybersecurity. Zhou Ningnan is an assistant researcher of Institute of Sci-Tech and Cyber Security at China Institutes of Contemporary International Relations (CICIR), whose research fields include cybersecurity.

The cybersecurity dilemma in the Asia-Pacific region is expected to further intensify, and the risk of cyber conflicts will continue to rise. This article analyzes the trend of NATO's eastward expansion of cybersecurity cooperation, focusing on strategic intention, impact, and prospects for expansion.

NATO's Cybersecurity Cooperation and Its Eastward Expansion

It is difficult for traditional military apparatus and practices to be effectively applied to the domain of cyberspace. Therefore, NATO's military coordination in cyberspace has certain particularities. Broadly, NATO's cybersecurity mechanism is a complex system that covers the extension of NATO's traditional military deployment in cyberspace. From a practical standpoint, however, NATO has long relied on the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE). Although NATO established the Cyberspace Operations Center in 2017, its role and influence are far less than that of CCDCOE, which is regarded by the network community as the core of NATO's network security mechanism.

CCDCOE is an organization for military cooperation among NATO member states and between member states and nonmember states. The initial goal of the center was to provide a platform for cyber-defense cooperation between NATO member states. In 2007, Estonia was hit by a large-scale cyberattack and did not receive substantial assistance from NATO member states on cyber-defense issues. At the time, NATO had not specified that the collective defense clause applied to cyberspace, nor did it have a cooperation mechanism in place for conducting cyber warfare. To address the lack of cooperation among NATO members in cyber warfare, then-General-Secretary of NATO Jaap de Hoop Scheffer adopted Estonia's proposal to establish a cyber-defense center. At the Bucharest Summit Declaration in April 2008, NATO members stated that NATO should further strengthen ties between member states and other countries and develop network defense capabilities.

In May 2008, the CCDCOE was established to foster cooperation of like-minded nations and partners and develop cyber-defense capabilities, and in October 2008, NATO granted it the status of international military organization. To avoid undue suspicion and alarm, the center's mission was

established as supporting member in cyber-defense research, training, and exercises with unique, interdisciplinary expertise in key technical, strategic, operational, and legal areas. The center is a voluntary organization established by various countries and recognized by NATO. It is not part of the NATO command structure, does not receive NATO funding, and does not directly participate in cyber operations. The center is formally separate from the NATO military command structure. In addition, cooperation is not limited to NATO member states and is not used as a formal military mechanism of NATO, which also facilitates CCDCOE flexibility and the further expansion of network military cooperation with nonmember states.

On a global scale, since cyber military cooperation involves highly sensitive military combat methods of various countries, the systematic cyber warfare cooperation resources owned by CCDCOE make it a rare cooperation partner for many parties. CCDCOE has organized cyber warfare lectures and tactics exchanges since 2008, and its accumulated cyber warfare resources have been affirmed by the United States, France, the UK, Spain, and other cyber powers. Former US Secretary of Defense Ashton Carter said that the CCDCOE's reserve of cyber warfare resources could play an important role in a world-class cyber war initiated by Russia.[1] CCDCOE also provides authoritative international legal and other policy support for cyber warfare. Since its establishment, CCDCOE has compiled several editions of the Tallian Manual to guide the US and other Western countries in cyber warfare and cyberattack activities, such as using force, countermeasures, and traceability in cyberspace. CCDCOE's research findings on cyber warfare and cyberattacks have been accepted by the US and other Western countries and translated into cyberspace position papers of these countries, which, in turn, have greatly influenced the UN's international position on cyberspace.

Because no NATO cyber military cooperation mechanism existed when CCDCOE was established, its goal is to become NATO's cyber military cooperation mechanism, providing guidelines for cyber warfare and cyberattacks. Even though NATO established the Cyberspace Operations Center in 2017 as a formal

[1] "US to Increase Contribution to Cooperative Cyber Defence, Secretary Carter Announces," https://ccdcoe.org/news/2015/us-to-increase-contribution-to-cooperative-cyber-defence-secretary-carter-announces/.

mechanism for cyber warfare collaboration among member states, it cannot replace the CCDCOE due to its short history. The CCDCOE is responsible for organizing cyber exercises and boosting NATO members' interoperability of cyber forces. To date, NATO still lists CCDCOE as an important cyber military agency.

After years of operations and maintenance, there are more CCDCOE members. Before its eastward expansion, it counted as members the 27 NATO member countries and four then European non-NATO countries (Austria, Finland, Sweden, and Switzerland). More recently, the CCDCOE has intensified its actions in the Asia-Pacific region, and its progressive eastward expansion has become increasingly evident.

First, South Korea, Japan, Australia, and New Zealand, NATO's original partners in the Asia-Pacific region, entered the game. As early as 2012, NATO signed Individual Partnership, and Cooperation Program agreements with Australia, New Zealand, and South Korea. However, given the international situation at that time, its priority areas of cooperation were mainly the maintenance of the rules-based international order, the Afghan issue, and the response to terrorism. With the increasingly fierce competition in cyberspace, however, NATO has adopted a three-step approach to promote practical cooperation with these partners in cyberspace.

The first step was conducting regular joint military exercises to lay a solid foundation for cooperation. Since 2012, NATO has held a cyber exercise called "Locked Shield," the world's largest cyber exercise, covering all offensive, and defensive exercises that may be involved in cyber warfare. Since 2019, Australia, South Korea, Japan, and New Zealand have successively participated in the "Locked Shield" exercise. Cyber-related departments and agencies of related countries, including the military, intelligence agencies, law enforcement agencies, critical infrastructure suppliers, and NATO member countries such as the US and the UK are participating in the exercise to demonstrate and exchange cyber offensive and defensive skills and to enhance joint military operational capabilities. The exercise focuses on the cooperation process, to enhance understanding, and trust. In 2021, Korea National Intelligence Service and Korea Electric Power Corporation formed a team of about 30 people to participate in the "Locked Shield" exercise. Officials from the National

Intelligence Service's Cyber Security Center expressed their interest in sharing cyber warfare-related skills with participating countries that have excellent cyber capabilities to strengthen the cooperation system.[1] Japan also sent teams from the Ministry of Defense, the Japan Computer Emergency Response Team Coordination Center, and critical infrastructure suppliers to participate in the exercise. An official from the Japan Computer Emergency Response Team Coordination Center said that the participation of Asia-Pacific countries in NATO cyber exercises deepened the collaborative relationship between Japan and the United States and other NATO member countries in cyber military, helping to build, and consolidate the cyber military cooperation system with NATO.[2]

The second step was to agree on strategic intentions and provide a strong support framework. In August 2019, NATO Secretary General Jens Stoltenberg visited Australia and New Zealand. He and the Australian Foreign Minister emphasized the importance of their cooperation in the cyber domain and noted cyber challenges as one of the three main areas for cooperation between NATO and New Zealand, along with great power competition and the threat of international terrorism.[3] In November of that year, NATO and South Korea signed an updated Individual Partnership and Cooperation Program, prioritizing cyber cooperation among the three key areas of cooperation. In 2022, against the backdrop of the Ukraine crisis, NATO Secretary General Jens Stoltenberg called for extending the shield against the aggression and fear created during the Cold War into cyberspace,[4] for elevating NATO's cyber military cooperation with Asia-Pacific partners, and for upgrading the cooperation framework with Asia-Pacific partners to the Individually Tailored Partnership Program to provide mechanisms to facilitate cyber military cooperation.[5]

---

[1] 원병철, "국정원, 세계최대규모사이버방어훈련 '락드쉴즈'첫참가, " https://www.boannews.com/media/view.asp?idx=96502.

[2] Koichiro Sparky Komiyama, "JPCERT/CC Participated in the Locked Shields 2022," https://blogs.jpcert.or.jp/en/2022/06/jpcertcc-participated-in-the-locked-shields-2022.html.

[3] "NATO Secretary General Begins Visit to New Zealand," https://www.nato.int/cps/en/natohq/news_168205.htm.

[4] "Keynote Address by NATO Secretary General Jens Stoltenberg at the NATO Cyber Defence Pledge Conference in Italy," https://www.nato.int/cps/en/natohq/opinions_208925.htm.

[5] Joint Statement Issued on the Occasion of the Meeting between H.E. Mr. Jens Stoltenberg, NATO Secretary General and H.E. Mr. Kishida Fumio, Prime Minister of Japan," https://www.nato.int/cps/en/natohq/opinions_211294.htm?selectedLocale=en.

The third step was to admit South Korea, Japan, Australia, and New Zealand as full members of the mechanism when the time was ripe. In 2022, the Korean National Intelligence Service and the Japanese Ministry of Defense announced their formal membership in CCDCOE, becoming the first Asia-Pacific countries to join the center in its 14 years of existence. The then head of CCDCOE, Merle Maigre, spoke of the significance of the Asia-Pacific partners officially joining the NATO cyber military cooperation mechanism, remarking on deepening the commitment to cyber military cooperation among like-minded countries. Japanese and South Korean public opinion also supports joining the NATO cyber military organization, considering it a milestone for cyber military cooperation with NATO. To enable these countries to better adapt to the mechanism, NATO has developed a new cooperation framework for Japan and South Korea, the Individually Tailored Partnership Program, to enable them to become NATO's closest partners in the cyber domain.

In addition to South Korea and Japan having completed the three-step process, Australia, and New Zealand are just one step away from concluding the process. There are already indications that NATO is lobbying. In March 2023, a military delegation from NATO's Cooperative Security Division visited Australia and New Zealand to sign the Individually Tailored Partnership Program with both countries, enhancing military consultations in the cyber domain and improving cooperation with NATO military operations.

Second, India, Singapore, and Thailand have also been recruited to join. Following incorporating Japan, South Korea, and other countries, NATO continued to attract more countries under the pretext of strengthening common defense, strengthening capacity building, and developing a so-called joint response to the threat posed by China. NATO's position is that India shares its will to confront China in cyberspace, regarding India as an important force for counterbalancing China in the Asia-Pacific region and cyberspace. Since the 2020 Sino–Indian border tensions, India has also begun to promote the "China Threat Theory" in cyberspace, claiming that China is responsible for the breakdown of India's power system during cyberattack events and other incidents. India's National Cyber Security Coordinator Rajesh Pant stated that China poses a major challenge to India's

cybersecurity. Despite India's long history of nonalignment, it has participated in the US–Japan–India–Australia Quadrilateral Security Dialog and has cooperated with the United States, Japan, and Australia on cyber issues. In August 2022, NATO's Allied Command Transformation published the Regional Perspectives Report on the Indo-Pacific, which stated that India has shown its willingness to cooperate with other countries and regions in the cyber field and that NATO should seize the opportunity to develop a partnership with India to jointly confront China in cyberspace.[1] On March 2, 2023, India, and NATO held an informal closed-door meeting during The Raisina Dialog, during which regional security issues including the Chinese cyber threat were discussed. NATO Secretary General Jens Stoltenberg has said that NATO is ready to engage with India and other Indo-Pacific countries to build tailored partnerships and further enhance comprehensive cybersecurity cooperation in the region.[2]

NATO and its member states have also strengthened cyber cooperation with Asia-Pacific countries such as Singapore and Thailand. In a May 2019 visit to Singapore, Maria Martens, President of the Science, and Technology Committee of NATO, stated that Singapore was threatened by so-called Chinese information warfare in cyberspace, that Singapore and NATO shared common cyberspace security concerns, and that both Singapore, and NATO were willing to cooperate in the cyber domain.[3] The United States and other NATO member states have also strengthened cyber military cooperation with the Asia-Pacific region. In February 2019, the US and Thailand conducted their first joint cyber exercise. Amorn Chomchoey, a Thai military official who participated in the exercise, reported that the exercise enhanced Thailand's cyber warfare awareness and technology, making Thailand aware of the pervasive nature of cyber warfare. In June 2022, the US and Philippine militaries communicated on cyber warfare tactics and cyber defense, followed by a strategic dialog in January 2023 to assess the Philippines' cybersecurity situation and agreement to engage in cyber defense cooperation. In October

---

[1] "Regional Perspectives Report on the Indo-Pacific," https://www.act.nato.int/download_file/view/2352.

[2] "Speech by NATO Secretary General Jens Stoltenberg at Keio University," https://www.nato.int/cps/en/natohq/opinions_211398.htm.

[3] "MISSION REPORT: Visit to Singapore," https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-11/202%20STC%2019%20E%20-%20Mission%20Report%20Singapore.pdf.

2022, after Singapore established its cyber forces—the Digital and Intelligence Service—the United States, a NATO member state, immediately conducted cyber dialogs with Singapore and organized officials from both sides' cyber forces for cyber-military cooperation. In November, the United States and ASEAN leaders issued a joint statement on cyber-military cooperation and added relevant content to the ASEAN Defense Ministers' Meeting Plus framework.

Third, NATO is trying to deploy cyber military forces in Taiwan. At present, Taiwan has carried out cyber military cooperation with NATO through different forms, such as sending personnel to participate in CCDCOE, participating in NATO cyber military policy discussions, and conducting so-called cybersecurity cooperation with the United States, Lithuania, and other NATO member states under the guise of preventing so-called Chinese cyberattacks. In August 2022, NATO's Allied Command Transformation reported that China was developing cyber weapons to isolate the Taiwan region, which would significantly impact NATO's security interests.[1] In September 2022, the Taiwan question was discussed at the NATO foreign ministers' meeting. Since then, NATO has begun to test the reactions of all parties to its cybersecurity meddling in the Taiwan question. On January 6, 2023, former NATO Secretary General and Danish Prime Minister Anders Fogh Rasmussen claimed during a visit to Taiwan that NATO should share cybersecurity intelligence, experience, and cooperation with Taiwan, and should jointly explore cyber defense cooperation.[2] Although there are still differences of opinion within NATO on the deployment of cyber military forces in Taiwan, as US Ambassador to NATO Julianne Smith said, it is enough for NATO to start discussing these questions.[3] It is expected that NATO will continue to promote cyber military cooperation with Taiwan in various ways in the future.

Under NATO's strategy of expanding its cyberspace alliance, its further expansion is likely. As the CCDCOE has stated, its vision is to foster cooperation among like-minded nations and to bring together NATO allies and partners

[1] "Regional Perspectives Report on the Indo-Pacific," https://www.act.nato.int/download_file/view/2352.

[2] Shelley Shan, "Europe Could Do More to 'Deter Attack' on Taiwan," https://www.taipeitimes.com/News/front/archives/2023/01/06/2003792076.

[3] Lili Bayer, "NATO's Looming Fault Line: China," https://www.politico.eu/article/nato-looming-fault-line-china/.

outside the alliance.[1]

Reasons for NATO's Eastward Cybersecurity Cooperation Expansion

The reason why NATO's security cooperation network's eastward expansion has progressed in recent years is mainly due to the maturity of the timing and the availability of objective conditions, and the outbreak of the Ukraine crisis has played a catalytic role in it.

First, the US is promoting a shift in the focus of NATO's cyber strategy to the Asia-Pacific. As early as 2008, NATO member states at the Bucharest Summit Declaration that NATO adopted a cyber-defense policy with the goal of further strengthening the links between member states and with other countries and enhancing cyber-defense capabilities.[2] Under the active leadership and promotion of the United States, NATO's cyber strategy, and policy began to pay more attention to the Asia-Pacific region, considering China, Russia, and other countries, especially China, as strategic adversaries to be countered and contained.

In 2019, the Trump administration called for confronting China in the cyber domain as a NATO priority at the Meeting of NATO Ministers of Foreign Affairs, and shortly thereafter at the London Summit, NATO members catered to US demands by emphasizing cyber cooperation with the United States to address the matter of China. NATO Secretary General Jens Stoltenberg has repeatedly claimed that NATO and its Asian partners face cyber threats from China, which is using its cyberattack capabilities to coerce NATO partners such as Japan and South Korea.[3] The CCDCOE report states that China's activities in cyberspace are a challenge to the security interests of NATO and its Asia-Pacific partners, and that China seeks to use cyber warfare capabilities to gain an advantage against NATO and its Asia-Pacific partners.[4] Therefore, addressing the so-called Chinese cyber threat should become a common

---

1 "Our Mission & Vision," https://ccdcoe.org/about-us/.

2 "Bucharest Summit Declaration," https://www.nato.int/cps/en/natolive/official_texts_8443.htm.

3 "Press Conference by NATO Secretary General Jens Stoltenberg," https://www.nato.int/cps/en/natohq/opinions_197292.htm.

4 A. Ertan, K.Floyd, P.Pernik, and T.Stevens, "Cyber Threats and NATO 2030: Horizon Scanning and Analysis," *NATO CCDCOE Publications*, December 2020, 141.

strategic objective of NATO and its Asia-Pacific partners.[1] After the Biden administration took office, the United States further raised the importance and urgency of its strategic competition with China. For example, the 2023 US National Cybersecurity Strategy proposes that cyberspace is at a turning point in what is considered a decisive decade in the strategic competition with China, seen as the most active and persistent threat to the US government and society and the only country with both the will and the power to reshape the international order. The smear campaign against China has also expanded from cyber espionage to the domination of emerging technologies critical to global development and export of digital authoritarian visions.[2] Therefore, strengthening of containment of China through the NATO framework is consistent with US strategic objectives and its interest in continued eastward expansion.

The US has leveraged the Taiwan situation to ramp up the urgency of NATO's eastward expansion. For example, in 2022, the US Senate passed the Taiwan Policy Act of 2022, claiming that the US has a responsibility if Taiwan was under oyber threat. US senior cyber official Jen Easterly exaggerated the cyber threat to Taiwan.[3] At a NATO meeting of foreign ministers in Bucharest in November 2022, US Ambassador to NATO Julianne Smith requested that NATO strengthen its cyber defenses and deepen relations with Asia-Pacific countries. After the meeting, the UK's ambassador to NATO, David Quarrey, stated that an evident reason for NATO's eastward expansion in cyberspace is the willingness of the United States to intervene in the Taiwan region.[4]

It is under the vigorous promotion of the United States that NATO's strategic shift has become clearer, reflected in the NATO 2022 Strategic Concept released in June of that year. The strategic document emphasizes that cyberspace is constantly competing, the Asia-Pacific region is vital to NATO, and NATO will strengthen dialog and cooperation with new and old partners

---

1 Marcos Perestrello, "NATO and the Indo-Pacific Region," https://www.nato-pa.int/document/2022-nato-and-indo-pacific-region-report-krimi-021-pcnp.

2 "National Cybersecurity Strategy," https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

3 Jeff Seldin, "US Warns of Massive Chinese Cyberattacks in Taiwan Scenario," https://thepressunited.com/news/us-warns-of-massive-chinese-cyberattacks-in-taiwan-scenario/.

4 Lili Bayer, "NATO's Looming Fault Line: China," https://www.politico.eu/article/nato-looming-fault-line-china/.

in the Asia-Pacific region to address cross-regional challenges and common security interests. The document also states that the Indo-Pacific region will increasingly affect the future of NATO and that the transatlantic region may become a secondary battlefield.[1]

Second, Japan, South Korea, and other countries have made full preparations to meet the important strategic shift of NATO's eastward expansion. Japan's new Cybersecurity Strategy announced in 2019 stated that China is Japan's primary cyber threat. Australia's then prime minister Scott Morrison stated that China considers Australia an important target for cyberattacks. Australia has also participated in collective traceability activities against so-called Chinese cyberattacks. Although South Korea has not yet stated that China is a cyber threat, it has continuously accused Chinese hackers of launching cyberattacks in recent years. The so-called China threat has been made into a common security concern between NATO and related countries.

To maximize cooperation with NATO in cyber defense, Japan, South Korea, and other countries have engaged in preparations to develop cyber forces and improve cyber military policies during 2019–2020. The Korea National Security Research Institute and the National Institute for Defense Studies under Japan's Ministry of Defense have sent staff to CCDCOE to learn the latest policy trends from NATO. At the same time, the Japanese government clarified in May 2019 that the country has the right to self-defense in cyberspace. In March 2022, Japan's Self-Defense Force launched a cyber-defense unit to centralize the command of Japan's cyber forces. The new National Security Strategy of Japan 2023 adopts the concept of "Active Cyber Defense" to take the lead in cyberattacks, and plans to grow its cyberattack force to 5,000 people within five years, which is comparable to the size of the cyber force of the US Cyber Command. South Korea is also reforming its cyber operations command mechanism in 2019, with the Joint Chiefs of Staff of the Republic of Korea unifying the command of cyber forces across the military services. Japan's and South Korea's cyber army construction has increased their likelihood of joining forces with NATO to conduct cyber defense operations,

[1] Sommet de Madrid, "The Madrid Strategic Concept and the Future of NATO," https://www.nato.int/docu/review/articles/2022/06/02/the-madrid-strategic-concept-and-the-future-of-nato/index.html.

which has been recognized by the United States and other NATO members. Furthermore, Japan, South Korea, and other countries have participated in operational military exercises with NATO members to comprehensively enhance interoperability with NATO regarding cyber military coordination, intelligence sharing, and technical cooperation.

Third, the Ukraine crisis has provided an opportunity for a breakthrough. After NATO's Asia-Pacific partners Japan and South Korea applied to join the CCDCOE in 2018, hoping to carry out cyber defense cooperation under the NATO framework, the outbreak of the Ukraine crisis offers a favorable opportunity to finalize this process.

The outbreak of the Ukraine crisis has further deteriorated the cybersecurity situation. Frequent cyberattacks between Russia and Ukraine have triggered a large number of cyberattacks around the world. For example, Ukraine has recruited approximately 300,000 hackers worldwide to form a cyber IT Army, and many hacker organizations such as KillNet have also appeared in Russia. To mobilize these hackers, Russia and Ukraine claim that the cyberattacks of so-called ethical hackers fighting for the country will not be legally punished. In addition to Russia and Ukraine, the United States, Belgium, and other countries also condone domestic hackers for launching cyberattacks, claiming that these hackers will not be prosecuted for cyberattacks launched in "good faith." Unchecked hacker behavior has caused a general deterioration of the global cybersecurity environment. Jason Healey, the drafter of the US National Cybersecurity Strategy in 2023, argues that Ukraine's campaign to legitimize hacking has eroded 20 years of global efforts to promote norms of responsible behavior in cyberspace, making cyberspace even less secure. In November 2022, the EU committee published the latest EU Cyber Defense Policy, stating that the EU should improve cyber defenses and strengthen international cyber cooperation to address the deteriorating cyber environment since the Ukraine crisis.[1]

Cyber warfare in the Ukraine crisis has, to a certain extent, underscored the effectiveness of cybersecurity cooperation. Prior to the Ukraine crisis,

[1] "Cyber Defence: EU Boosts Action against Cyber Threats," https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642.

cyberspace was widely perceived as easy to attack but difficult to defend, and cyberattacks were considered an effective asymmetric tool that were difficult to prevent. Former director of US national intelligence James Clapper gave a graphic illustration of cyberwarfare's offensive and defensive asymmetries at a congressional hearing, comparing cyberattacks to rocks, and cyber defense to glass houses.[1] US cyber warfare expert at the RAND Corporation William Courtney believes that Russian cyberattacks on Ukraine are difficult to prevent and will cause damage to Ukraine's critical infrastructure and military equipment.[2] The US government is also concerned that Russia could launch cyberattacks in the war with the aim of destroying modern, digital military equipment. However, no public reports have confirmed that cyberattacks on either side have damaged military equipment. Gavin Wilde, a researcher in the Carnegie Endowment for International Peace, argues that while both sides may have concealed the incident, the fact that both sides were able to conceal it for so long underscored that the cyberattack did not have the desired effect.[3] Therefore, the cyber community generally believes that Ukraine's defense against Russian cyberattacks was successful and that the importance and effectiveness of its cyber defense was validated. This judgment has to some extent reversed the international community's perception that cyberattacks are easier to execute than cyber defense.

Victor Zhora, Deputy Chairman, and Chief Digital Transformation Officer at the State Service of Special Communications and Information Protection of Ukraine, reported that the Ukraine National Power Company Ukrenergo was attacked by sophisticated Russian cyber weapons, nearly causing a loss of power to 2 million people. However, the Slovak cybersecurity company ESET detected and dealt with the cyberattack in time, avoiding a catastrophic impact. Former US national cyber director Chris Inglis said that if a country cooperates in international cybersecurity, a successful cyberattack against it would

---

[1] James Clapper, "Statement for the Record Worldwide Cyber Threats," https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2015/item/1251-dni-clapper-statement-for-the-record-worldwide-cyber-threats-before-the-house-permanent-select-committee-on-intelligence.

[2] William Courtney and Peter Wilson, "If Russia Invaded Ukraine," https://thehill.com/opinion/international/584805-expect-shock-and-awe-if-russia-invades-ukraine/?rl=1.

[3] Gavin Wilde, "Cyber Operations in Ukraine: Russia's Unmet Expectations," https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607.

simultaneously require defeating the cyber defense capabilities of each country.[1] Jon Bateman, a researcher at the Carnegie Endowment for International Peace, argues that if a country does not have the same cyberattack capabilities as the United States, the development of cyberattack weapons may not pay off, and that international cybersecurity cooperation could be effective against national cyberwarfare.[2]

The crisis in Ukraine has further reinforced the need for cybersecurity cooperation between NATO and its Asia-Pacific partners. At the beginning of the Ukraine crisis, Japan announced its support for Ukraine and imposed economic sanctions on Russia. Considering possible cyber retaliation, Japan's Ministry of Economy, Trade and Industry issued a notice on the same day of the sanctions against Russia, urging relevant ministries, and companies to take measures to deal with possible cyberattacks. South Korea also claimed that it suffered large-scale, high-level cyberattacks during this period. As the Director of NATO's cyber exercise Charles Elliott said, the crisis in Ukraine has led to an increased need for NATO's cyber defense cooperation.[3] Japan and South Korea have taken advantage of the shared concern expressed by domestic and foreign public opinion about cyberattacks, removing the greatest potential policy doubts and obstacles and completing the final step of joining CCDCOE.

During the Ukraine crisis, Ukraine has shared significant amounts of information on cyberattacks with NATO, with the head of CCDCOE reporting that this first-hand information has been very valuable.[4] NATO believes that the future of cyber threats will originate not only from Russia, but also from China, the DPRK, and other countries. In the future, both the United States, and US-led NATO will need to increase cooperation with Asia-Pacific partners to obtain more first-hand information to help strengthen their advantage over China in cyberspace. Thus, NATO views promoting cybersecurity cooperation

---

[1] Kirsten Errick, "At DEF CON, National Cyber Director Chris Inglis Discussed the Nuances of Cyber Defense," https://www.nextgov.com/cybersecurity/2022/08/white-house-cyber-director-defense-new-offense-cyber/375822/.

[2] Jon Bateman, Nick Beecroft, and Gavin Wilde, "What the Russian Invasion Reveals about the Future of Cyber Warfare," https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667.

[3] Maggie Miller, "NATO Prepares for Cyber War," https://www.politico.com/news/2022/12/03/nato-future-cyber-war-00072060.

[4] Daryna Antoniuk, "Ukraine Signs Agreement to Join NATO Cyber Defense Center," https://therecord.media/ukraine-signs-agreement-to-join-nato-cyber-defense-center.

eastward urgently.

Prospects for Eastward Expansion of NATO Cybersecurity Cooperation

The eastward expansion of NATO cybersecurity cooperation is an important NATO initiative for cyber deterrence in the Asia-Pacific region, especially for strategic containment of China, which has adversely impacted the region and global cybersecurity more generally. Although it has progressed, the subsequent development still depends on all parties and faces greater uncertainty.

First, the ultimate strategic objectives are different. NATO's objective in eastward expansion is mainly to counter China; thus, more emphasis is placed on strengthening military cooperation, joint operations, and cyber deterrence through a collective defense posture. Although some countries in the Asia-Pacific region have followed up on the "Chinese cyber threat theory" in their China strategies, their ultimate goal is not entirely to contain China, but rather to use this mechanism to improve their own cybersecurity capabilities and better safeguard their own cybersecurity interests.

South Korea released its National Cybersecurity Strategy in 2019, proposing to strengthen the ability to repair core infrastructure in the event of cyberattacks and build a future-oriented cybersecurity system that encompasses all areas of the civil, government, and military sectors based on mutual trust among individuals, companies, and the government. Australia's Cyber Security Strategy 2020 proposed addressing the security issues faced by businesses and individuals working remotely and improving the security of critical information and communications technology infrastructure security. The cybersecurity strategies of these countries prioritize the cybersecurity of their own critical infrastructures and take defensive measures, such as strengthening government cooperation with the public and enterprises and enhancing cybersecurity situational awareness as the foundation for implementing cyber strategies.

Since the Ukraine crisis outbreak, especially the cyber conflict, the Asia-Pacific region has realized that the best way to deal with cyberattacks is not cyber deterrence, but to enhance the defensive capabilities and resilience of its own cyber systems. For example, the 2023–2030 Australian Cyber

Security Strategy is based on Australia's Cyber Security Strategy 2020 to strengthen cyber capacity building, which began emphasizing building critical infrastructure for security and resilience and improving government and enterprise network security threat sharing and blocking mechanisms.[1] Therefore, compared with NATO's offensive approach, Asia-Pacific countries are more inclined to adopt a defensive approach.

Second, the countries involved have doubts about militarizing cyberspace. NATO's cyberspace operation mode is shifting from a traditional common defense posture to jointly conducting cyberattacks. Since 2018, CCDCOE is no longer satisfied with organizing cyber exercises focused on cyber defense, but has instead started to organize cyber exercises concerning cyberattacks. Especially after the crisis in Ukraine, its aggression has become more evident. In April 2023, Prime Minister Kaja Kallas of Estonia, the founding country of CCDCOE, demanded that Russia be punished in cyberspace regarding the Ukraine crisis. This statement is seen as the latest signal of the transformation of NATO's cybersecurity mechanism to one of cyberattacks. This has somehow increased the suspicion of some countries that do not want to be held hostage to a larger conflict. For example, since 2018, Estonia has held several rounds of high-ranking official exchanges with India, promising to provide cybersecurity-building resources to India in the hope that India will join CCDCOE; nevertheless, India has still not clarified its position. Meanwhile, India has actively participated in cyber offensive and defense exercises hosted by the UK, but has not participated in CCDCOE's cyber exercises. It is expected that if NATO goes further down the road of cyberattack and deterrence, the strategic doubts, and decision-making pressures of the relevant Asia-Pacific countries will grow.

Third, the so-called cybersecurity shelter that can be offered to the countries concerned is limited. NATO's cybersecurity mechanism is still immature, especially the core of NATO's cyber deterrence strategy; its collective defense mechanism has always been difficult to activate to provide direct help to Asia-Pacific partners. In addition, NATO's Asia-Pacific partners

[1] "2023-2030 Cyber Security Strategy Discussion Paper," https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf.

are not NATO members, and thus, are ineligible to invoke NATO's collective defense provisions in the event of a cyberwarfare attack. Even if NATO can provide its Asia-Pacific partners the same treatment as member states on the issue of cybersecurity protection, it has proven difficult for the Asia-Pacific partners to obtain substantial cybersecurity guarantees. In July 2022, Algeria was subjected to a cyberattack that was immediately investigated by the United States, NATO, and Algeria, which determined that they breached Article 5 of the NATO treaty. Algeria sought the use of Article 5 of the NATO treaty from NATO. The necessary conditions for NATO to initiate collective defense provisions against this round of cyberattacks are all in place, but ultimately unfulfilled. NATO has worries about granting cybersecurity sanctuary to its members, making it more difficult to provide substantive help to its Asia-Pacific partners.

Fourth, it is difficult for the network resources provided by NATO to meet the expectations of relevant Asia-Pacific countries, which have great practical demands in terms of network defense and security capacity building, especially network offensive, and defensive technology exchanges and information sharing, so they can carry out multidimensional cooperation in strategy, policy, technology, and information under the NATO mechanism. In the long run, however, it is difficult to meet expectations. The cyber warfare resources that NATO has long hoarded have been tested in actual combat and are not as advanced as imagined. For example, after NATO cybersecurity agencies such as CCDCOE exchanged experiences on cyber warfare with Ukraine, Tom Kellermann, the former commissioner on the Commission on Cyber Security for the 44th President of the United States, said, NATO's ability to improve its defenses against Russian cyber warfare depends on lessons learned from Ukraine.[1] The EU has also emphasized the need to strengthen its network capacity building and achieve independent network defenses, indicating that it is uncomfortable relying entirely on NATO security mechanisms. Moreover, NATO has limited cyber situational awareness in the Asia-Pacific region. Practice has shown that NATO is ineffective at helping Asia-Pacific

[1] Jessica Lyons Hardcastle, "Ukraine Slides Closer to NATO with Buckets of Experience Fending off Moscow's Cyberattacks," https://www.theregister.com/2023/01/24/ukraine_nato_cyber_defense/.

partners deal with cybersecurity threats. For example, in the face of multiple cyberattacks on South Korea, Japan, and Australia, NATO provided only limited resources, and these countries eventually chose to seek help directly from the United States, the United Kingdom, and other countries. Therefore, in the long run, how far the cooperation between NATO and Asia-Pacific member countries can go depends on the extent to which the support provided by NATO effectively meets the demands and expectations of the relevant countries.

Conclusion

The impact of the eastward expansion of NATO's security cooperation network to address cybersecurity has already appeared, causing widespread concern in other countries in the Asia-Pacific region about the deterioration of the security situation. In the view of Japan, South Korea, Australia, and other countries enhancing their cyber military capabilities and cooperation with NATO, Asia-Pacific countries such as India, Singapore, Malaysia, the Philippines, and Vietnam have also increased their investment to improve their own security, establishing, and expanding network forces. Relevant countries have also developed and purchased large numbers of cyber weapons and organized and participated in large-scale cyber exercises, contributing to intensifying the cyber arms race in the Asia-Pacific region. Under such circumstances, cyberspace has misfired, the risk of conflict escalation has been rising, and the security dilemma has become more acute.

At the same time, NATO, and its partners in the Asia-Pacific have strengthened cyber-military cooperation. The strategic influence exerted by the US through NATO is not limited to the military field, but will serve the United States' interest in building a cyberspace alliance system to further contain and suppress China and prevail in the strategic competition.

Thus, China should attach great importance to these developments. First, it should recognize the crucial importance of NATO's network security cooperation eastward expansion from a strategic perspective, especially the adverse impact on China's surrounding network security environment. Second, China should carry out active countermeasures, not to engage in simple cyber confrontation, but rather to strengthen its own cybersecurity

situational awareness and cyber-defense capabilities in a targeted manner while comprehending the needs of countries in the Asia-Pacific region to strengthen cybersecurity capacity building, strengthen cooperation, provide quality cybersecurity public goods, and hedge against NATO's influence in the region. Third, China should strengthen its agenda-setting at the international level, continue to oppose arms competition and militarized development in cyberspace, encourage the international community to pay attention to and be alert to this trend, and shape an international public opinion environment conducive to the peaceful and stable development of cyberspace.