MAIAC

NORTH ATLANTIC TREATY ORGANIZATION (NATO)
BACKGROUND GUIDE

MID-AMERICAN INTERNATIONAL AFFAIRS CONFERENCE
DECEMBER 1-2, 2023

PRESENTED BY

MAGEC

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

A. A TRANSATLANTIC STRATEGY ON CHINA

Throughout NATO's history, alliance members have held differing views on China and the security challenges posed by its rising influence. Many European members rely heavily on Chinese trade and investment and have no security obligations in Asia, while the United States holds defense commitments with a number of Asian countries, complexifying its relationships in the region.

Despite differing perspectives, the Alliance recently reached a consensus on key emerging security concerns; in June 2022, for the first time in NATO's history, China was addressed in NATO's Strategic Concept as a "challenge to our interests, security, and values."[1] The Strategic Concept outlined a number of issues, including: 1) China's enhanced security ties with Russia, 2) China's efforts to control key technological and industrial sectors, 3) human rights abuses and coercive authoritarian policies (e.g., abuses in Hong Kong and an increasingly aggressive position toward Taiwan), and 4) subversion of the rules-based international order.

Implementing NATO's China position entails increasing intelligence sharing, mitigating the risks of supply chain and technological reliance for defense, and promoting ongoing freedom of navigation operations, among other efforts.[2] NATO members have asserted that they remain open to constructive engagement with China, while simultaneously underscoring the importance of strengthening other Indo-Pacific partnerships.

---

[1] NATO Strategic Concept, 29 June 2022, Madrid, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

[2] Binnendijk, Hans, Hamilton, Daniel S, The Atlantic Council, "Implementing NATO's Strategic Concept on China", https://www.atlanticcouncil.org/in-depth-research-reports/report/implementing-natos-strategic-concept-on-china/#:~:text=%5BTo%20implement%20NATO's%20Strategic%20Concept,of%20navigation%20operations%20in%20Asia, 2 February 2023

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

B. CYBER DEFENCE

On November 10, 2022, NATO Secretary General Jens Stoltenberg stated, "In 1949, President Truman described NATO as 'a shield against aggression and the fear of aggression.' Today, that shield extends to cyberspace. The threat from cyberspace is real, and it is growing" in his keynote address at the NATO Cyber Defence Pledge Conference in Rome, Italy.[3] As the alliance moves into the twenty-first century and beyond, it is vital that its support of the collective defense extend beyond boots-on-the-ground conflicts to those that are almost purely digital.

Given its many facets and high level of technicality, cybersecurity is an often misunderstood topic. At its simplest, cybersecurity is the art of protecting one's devices and information from malicious actors who wish to access or even manipulate them. At the national level, this includes protecting both personal and large-scale technologies from domestic and international actors who wish to do the nation harm. It is important to recognize, though, that cyber security at the national and international level is exponentially more complex than the personal level.[4]

While the North Atlantic Council, NATO's main political decision making body, does guide the alliance's cyber defense efforts, much of the actual policy comes from the Cyber Defense Committee. It is this body that oversees NATO's own cyber security (through the NATO Cyber Security Centre), along with supporting that of its member states. To ensure its systems and personnel are properly trained, the alliance conducts regular exercises, including the annual Cyber Coalition Exercise, and incorporates cyber defense into its regular crisis management exercises. The alliance makes Cyber Rapid Reaction Teams available to allies, further recognition that NATO's cyber defense relies on the international community as a whole, including non-NATO allies.[5]

Established on May 14, 2008, the majority of NATO's cybersecurity expertise is housed within the Cooperative Cyber Defence Centre of Excellence ("CCDCOE"). Made up of an administrative arm, technology branch, strategy branch, operations branch, law branch, education and training branch, and support branch, the CCDCOE acts as a multifunctional and multidisciplinary body, recognizing the complex nature of cybersecurity. Since 2009, the CCDCOE has hosted the annual International Conference on Cyber Conflict, known as CyCon. Bringing together cybersecurity professionals, academic researchers, and government officials, CyCon has become a staple of the

[3] https://www.nato.int/cps/en/natohq/opinions_208925.htm
[4] https://www.cisa.gov/news-events/news/what-cybersecurity
[5] https://www.nato.int/cps/en/natohq/topics_78170.htm

cyber defense community. It should be noted that the CCDCOE's efforts are not just limited to benefiting NATO, with 8 "Contributing Participants" outside the alliance (Austria, Australia, Ireland, Japan, South Korea, Sweden, Switzerland, Ukraine), along with countless relations with other non-NATO states, universities, research institutions, and businesses.[6]

[6] https://ccdcoe.org/about-us/