North Atlantic Treaty Organization (NATO)

Last Updated: September 2020

Member States

POLICY

Strategy Documents

Enhanced Cyber Defence Policy (not published)

Heads of State and Government

• Clarifies that a major digital attack on a member state could be covered by Article 5 of the North Atlantic Treaty;
• Further improves information-sharing and mutual assistance between Allies, enhances training and exercises and furthers cooperation with the industry.

Source

5 September 2014 (approved on)

2018 Brussels Summit Declaration

Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018

- Addresses cyber threats (para. 20);
- Identifies cyber defence as part of NATO's core task of collective defence;
- Reaffirming NATO's defensive mandate, determined to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign.

Source

11 July 2018

Other Documents

Tallinn Manual 2.0

CCDCOE

- Document issued by CCDCOE, affiliated entity - not officially endorsed by Allies;
- Comprehensive analysis of how existing international law applies to cyberspace and the more common cyber incidents that states encounter on a day-to-day basis;
- The Original Tallinn Manual focused mainly on the most severe cyberoperations, those violating the prohibition of the use of force in international relations.

Source Source 2

2017

Communications

Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity

ITU, the World Bank, Commonwealth Secretariat, Commonwealth Telecommunications Organisation, NATO CCD COE

• Co-publication aiming to guide national policy-makers in the development of a national cybersecurity strategy;
• Provides an overview of a strategy development lifecycle, overarching principles for a strategy, focus areas and good practices, and supporting reference materials.

Source

2018

Cyber Defence Pledge

Heads of State and Government

Pledge by the Allied Heads of State and Government to strengthen and enhance the cyber defences of national networks and infrastructures as a matter of priority.

North Atlantic Treaty Organization (NATO)

Last Updated: September 2020

Source

8 July 2016

Wales Summit Declaration

Heads of State and Government

• Endorsed an Enhanced Cyber Defence Policy, which reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence;
• Recognizes that international law applies in cyberspace;
• Affirms cyber defence as part of NATO's core task of collective defence.

Source

5 September 2014

STRUCTURE

Specialized Agencies

NATO Communications and Information Agency

NATO Communications and Information Organization

- Responsible for connecting the Alliance, defending its networks, and providing rapid support to NATO operations and missions;
- Tasked with delivering critical capabilities, including: the command and control technology for NATO's ballistic missile defence, the Air Command and Control System, support to NATO's Joint ISR Initiative and Federated Mission Networking;
- Runs the NATO Computer Incident Response Capability (NCIRC), providing round the clock protection of NATO networks.

Source

1 July 2012

North Atlantic Council

- Provides high-level political oversight on all aspects of the implementation of the NATO Policy on Cyber Defence;
- Apprised of major cyber incidents and attacks, and
- Exercises principal authority in cyber defence-related crisis management.

Source

Cyber Defence Committee

North Atlantic Council

Lead committee for political governance and cyber defence policy in general, providing oversight and advice to Allied countries on NATO’s cyber defence efforts at the expert level.

Source

NATO Cyber Defence Management Board

- Responsible for coordinating cyber defence throughout NATO civilian and military bodies;
- Comprises the leaders of the policy, military, operational and technical bodies in NATO with responsibilities for cyber defence.

Source

NATO Consultation, Control and Command (NC3) Board

Constitutes the main committee for consultation on technical and implementation aspects of cyber defence.

North Atlantic Treaty Organization (NATO)

Last Updated: September 2020

Source

NATO Military Authorities

Bear the specific responsibilities for identifying the statement of operational requirements, acquisition, implementation and operating of NATO's cyber defence capabilities, along with the NATO Communications and Information Agency (NCIA).

Source

Allied Command Transformation

Responsible for the planning and conduct of the annual Cyber Coalition Exercise.

Source

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

- Affiliated entity - not part of NATO structure;
- Supports its member nations and NATO with cyber defence expertise in the fields of technology, strategy, operations and law;
- Organizes Locked Shields, the world's largest and most complex international technical cyber defence exercise;
- Organizes the annual conference on cyber conflict, CyCon;
- Not part of NATO's military command or force structure.

Source

Key Positions

Director, NATO Cooperative Cyber Defence Centre of Excellence

Source

General Manager, NATO Communications and Information Agency

Source

LEGISLATION

COOPERATION

Meetings

NATO Information Assurance Symposium (NIAS)

NATO's largest cyber conference on the critical role cyber security plays in securing the Alliance.

Source

NATO Annual Cyber Coalition Exercise

North Atlantic Treaty Organization (NATO)

Last Updated: September 2020

- Annual exercise testing and training cyber defenders from across the Alliance in their ability to defend NATO and national networks involving around participants from Allies, partners, industry and academia;
- Aims to enhance coordination and collaboration between NATO and Allies, strengthen the ability to protect Alliance cyberspace, and conduct military operations in the cyber domain.

Source

International Conference on Cyber Conflict

NATO CCDCOE

• Organized annually since 2009;
• Hosts all the focus areas of cyber conflict in a single event, allowing in-depth discussions on specific topics related to technology and malware development, education and training issues, legal aspects, etc.

Source

2009 (first conference)

Activities

Critical Information Infrastructure Protection Course

CCDCOE

- Provided by CCDCOE, entity affiliated to NATO;
- Unclassified course intended for mid-level managers responsible for the protection of critical information infrastructure.

Source

2018 (since)

Executive Cyber Seminar

NATO CCDCOE

- Provided by CCDCOE, entity affiliated to NATO;
- Course for senior level staff for whom cyberspace is a new area of responsibility or consideration.

Source

2017 (since)

Technical Courses

NATO CCDCOE

- Provided by CCDCOE, entity affiliated to NATO;
- Technical courses organized twice a year with an aim to bring together and train computer and network security specialists.

Source

2015 (since)

Law Course

NATO CCDCOE

- Provided by CCDCOE, entity affiliated to NATO;
- Offered twice per year, the course provides a practice-oriented survey of the international law applicable to cyber operations involving States.

Source

2014 (since)

North Atlantic Treaty Organization (NATO)

Last Updated: September 2020

Locked Shields
NATO CCDCOE

• Biggest and most advanced international live-fire cyber defence exercise in the world: scenario-based real-time network defence exercise focusing on training security experts who protect IT systems on a daily basis;
• Organized annually.

Source

2010 (first exercise)

External Cooperation

Project, NATO-Moldova
NATO Science for Peace and Security Programme

Multi-year project to establish the Moldovan Armed Forces Cyber Incident Response Capability with a supporting cyber defence infrastructure.

Source

13 Feb. 2018

Cooperation, Estonia/NATO-Japan

• Cooperation on cybersecurity;
• Japan to join the NATO-accredited cyber defence hub (NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE) based in Tallinn.

Source

12 Jan. 2018

Cooperation Agreement, EU-NATO
EU Ministers

Agreement to step up cooperation between the two organisations in a number of areas, including cyber security and defence

Source

8 december 2017

NATO-Kuwait ICI Regional Center activities

Includes cooperation in cyber defence

Source

17-20 September 2017

Agreement, NATO-Lithuania

Agreement enhancing Lithuanian and NATO cooperation in cyber security.

Source

6 Jul. 2017

Cooperation, NATO-Bosnia and Herzegovina

North Atlantic Treaty Organization (NATO)

Last Updated: September 2020

Exploration of common solutions to security challenges in the arae of cyber defence during the Science for Peace and Security (SPS) Programme Information Day

Source

19 May 2017

Morocco-NATO Talks

• Cooperation in the field of countering cyber security risks at the heart of the talks;
• Examination of future cooperation prospects in cyber security.

Source

18 May 2017

EU-NATO (15283/16)

European Council

Council Conclusions on the Implementation of the 8 July 2016 EU-NATO Joint Declaration.

Source Source 2

6 december 2016

NATO Training

Training to improve expertise and technical knowledge and to contribute to the strengthening of Iraqi national cyber defence capabilities

Source

November-December 2016

Memorandum of Understanding, Bulgaria-NATO

Facilitate information-sharing on cyber threats and best practices, improve the prevention of cyber incidents and increase Bulgaria's resilience to cyber threats

Source

26 Oct. 2016

Memorandum of Understanding, Iceland-NATO

Permanent Representative of Iceland to NATO

Memorandum of Understanding on cyber defence cooperation.

Source

18 Oct. 2016

Memorandum of Understanding, Portugal-NATO

Second generation Memorandum of Understanding, aims to further improve cyber defence cooperation and assistance between NATO and national cyber defence authorities.

Source

14 Jul. 2016

North Atlantic Treaty Organization (NATO)

Last Updated: September 2020

Memorandum of Understanding, Slovenia-NATO

Memorandum of Understanding on cyber defence cooperation.

Source

10 May 2016

EU-NATO Technical Arrangement

NATO Computer Incident Response Capability (NCIRC); CERT-EU

Facilitates technical information sharing between NCIRC and CERT-EU to improve cyber incident prevention, detection adn response in both organisations, in line with their decision making autonomy and procedures.

Source

10 Feb. 2016

NATO Science for Peace and Security (SPS) project to enhance Jordanian cyber defence capabilities

Includes 2017 establishment of CERT team; follow-up multi-year project is currently under development

Source

2014

NATO-Ukraine Trust Fund for Cyber Defense

• Provides Ukraine with the necessary support to develop its strictly defensive, CSIRT-type technical capabilities, including laboratories to investigate cybersecurity incidents;
• Training and advisory dimension based on the interests of both Allies and Ukraine derived from the requirements of Ukraine's security and defence sector institutions.

Source

december 2014

Discussions, Slovakia-NATO

• Meeting on NATO defense planning process;
• Included discussions on cyber security.

Source

5 Jun. 2013

Memorandum of Understanding, NATO-Czech Republic

Concerning cooperation on cyber defence

Source

14 Mar. 2012

Memorandum of Understanding, Romania-NATO

Memorandum of Understanding with NATO Cyber Defence Management Board to increase cooperation on cyber security.

Source

North Atlantic Treaty Organization (NATO)

Last Updated: September 2020

18 Oct. 2011

Memorandum of Understanding, Lithuania-NATO

- Memorandum of Understanding for Cooperation in Cyber Defence with NATO;
- Participates in various NATO cyber exercises such as Cyber Coalition, Crisis Management Exercise CMX, and others.

Source

Summer 2010