



Documentos

NATO

Cyber Defence Pledge

8 July 2016, Warsaw, Poland

1. In recognition of the new realities of security threats to NATO, we, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea.

2. We reaffirm our national responsibility, in line with Article 3 of the Washington Treaty, to enhance the cyber defences of national infrastructures and networks, and our commitment to the indivisibility of Allied security and collective defence, in accordance with the Enhanced NATO Policy on Cyber Defence adopted in Wales. We will ensure that strong and resilient cyber defences enable the Alliance to fulfil its core tasks. Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of Allied operations.

3. We welcome the work of Allies and the EU on enhancing cyber security, which contributes to reinforcing resilience in the Euro-Atlantic region, and we support further NATO – EU cyber defence co-operation, as agreed. We reaffirm the applicability of international law in cyberspace and acknowledge the work done in relevant international organisations, including on voluntary norms of responsible state behaviour and confidence-building measures in cyberspace. We recognise the value of NATO's partnerships with partner nations, industry and academia, including through the NATO Industry Cyber Partnership.

4. We emphasise NATO's role in facilitating co-operation on cyber defence including through multinational projects, education, training, and exercises and information exchange, in support of national cyber defence efforts. We will ensure that our Alliance is cyber aware, cyber trained, cyber secure and cyber enabled.

5. We, Allied Heads of State and Government, pledge to strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority. Together with the continuous adaptation of NATO's cyber defence capabilities, as part of NATO's long term adaptation, this will reinforce the cyber defence and overall resilience of the Alliance. We will:

I. Develop the fullest range of capabilities to defend our national infrastructures and networks. This includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks;

II. Allocate adequate resources nationally to strengthen our cyber defence capabilities;

III. Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen co-operation and the exchange of best practices;

IV. Improve our understanding of cyber threats, including the sharing of information and assessments;

V. Enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;

VI. Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance;

VII. Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends.

6. To track progress on the delivery of our Pledge, we task an annual assessment based on agreed metrics, and we will review progress at our next summit.