Communique 1.2 - Addressing Returning Terrorist Fighters and Deradicalization

Preamble:

Understanding that countries maintain their sovereignty in any alliance and value their national security in the face of these non-state actors,

Recognizing the limitations of rehabilitation policies,

Defining need to know basis as restricting data to that which a government requires to keep citizens safe within borders based on pre-emptive data to ensure timely deliverance,

Operative:

We, the Members of the Alliance:

1. *Encourage* states to implement policies that would prevent civilians from becoming radicalized;
2. *Make* use of existing intelligence-sharing frameworks both databases and centers of excellence including:
    a. Counter Intelligence;
    b. Human Intelligence;
    c. Defence Against Terrorism;
    d. Defence Against Terrorism Programme of Work.

Communiqué 2.1 - Addressing Hostile State Actors

Preamble:

Acknowledging the NATO priority to deter and defend allies and to mitigate the need to invoke Article 5 action,

Recognizing the threat of cyber-attacks and the concerns as it falls below the threshold of Article 5,

Recognizing the increasingly strategic and economic importance of the Arctic for NATO member states,

Welcoming the expertise and recommendations of the Counterintelligence Centre of Excellence and Cooperative Cyber Defence Centre of Excellence in the area of cyber defence,

Operative:

We, the Members of the Alliance:

1. *Recommend* greater investment in emerging technologies that improve the existing intelligence frameworks combatting state and non-state actor interference, by including but not limited to;
    1. Advanced secure wireless networks,
    2. Automated systems,
2. *Recommend* to update the Multinational Cyber Defence, Education and Training Centre wide curriculum on basic cyber knowledge, including but not limited to the following topics:
    1. Basic cyber hygiene and its importance,
    2. Knowledge on the use of security softwares,
    3. Basic knowledge of the cyber kill chain as defined by the company Lockheed Martin,
9. *Recommend* to expand the training of new network analysts employees and keep the training program for new analysts up to date to include training on a wider variety of cyber defence and analysis tools in order to accommodate the growth of networks in NATO country and increase in their network traffic;
10. *Encourage* the expansion of currently existing cyber security exercises to include many NATO countries.