Assessing and enhancing National Cyber Sovereignty
A Hands-on Framework
Assessing and enhancing National Cyber Sovereignty
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/ THE RATIONALE FOR CYBER SOVEREIGNTY</td>
<td>4</td>
</tr>
<tr>
<td>2/ ASSESSING A NATION’S CYBER SOVEREIGNTY</td>
<td>5</td>
</tr>
<tr>
<td>3/ THALES’ NATIONAL CYBER SOVEREIGNTY INDEX</td>
<td>6</td>
</tr>
<tr>
<td>4/ BUILDING YOUR NATION’S ROADMAP</td>
<td>7</td>
</tr>
<tr>
<td>5/ WORKING WITH THALES</td>
<td>8</td>
</tr>
<tr>
<td>CONTACT US</td>
<td>9</td>
</tr>
</tbody>
</table>
1. The Rationale for Cyber Sovereignty

For them to thrive peacefully, Nations need to be resilient to cyber-threats. Cyber Resilience creates cybersecurity (cyber-attack prevention) and cyber defence (cyber-attack resolution) capacities.

As attacks come in a wide variety of clever forms, capable of defeating best-in-class cybersecurity measures, Nations must seek to regain the initiative over cyber-enemies in a world of hyper connectedness and borderless global cyber-threat.

Cyber Sovereignty is all about this.

For instance, the Government’s cybersecurity agency, with the help of trusted, for instance defense-related, services or partners, creates secret attack signature detection capacities.

Those can then equip national critical infrastructure operators’ Intrusion Detection / Prevention Systems. Attackers knowing not about such a cyber defense advantage mount attacks that then get more easily detected and resolved.

KEY POINT

Cyber Sovereignty is a Nation’s aptitude to control the security & activity in the cyberspace across its territory and its activities abroad.

It helps protecting Nations to secure the Rule of Law and Peace, the country’s good governance, its national power, human rights, societal and economic continuity, or else sensitive data & secrets.

Finally, Cyber Sovereignty requires governmental cooperation and industry partnerships.
2. Assessing a Nation’s Cyber Sovereignty

A Nation’s journey towards Cyber Sovereignty takes account of a wide variety of factors. Politics and threats, the complex ecosystem of the governance of cyber, stakeholders’ cyber maturity, technological dependencies on foreign countries and the existence of national cyber resilience capabilities, to quote a few, all influence how fast and how far Cyber Sovereignty should and can be improved.

If the United Nations’ ITU Global Cybersecurity Index (GCI) measures the cybersecurity maturity of 193 countries over the Globe, a more specific assessment of a Nation’s Cyber Sovereignty can be made via Thales’ National Cyber Sovereignty Index™ (NCSI).

Based on 6 areas and 18 pillars, this index helps a Nation to assess where it starts from and the domains in which it needs to make progress.

**In Thales’ NCSI, the six areas are:**

1. National Cyber Strategy;
2. National Education & Training Strategy;
3. National Research & Technology Strategy;
4. Corporate Cyber Maturity Enhancement;
5. Sovereign Solutions & Technologies;
6. Governmental Capabilities.

**IMPORTANT NOTE**

The starting point of this journey towards excellence is the initial index of cyber sovereignty of the Nation.
3. Thales’ National Cyber Sovereignty Index

Thales’ National Cyber Sovereignty Index areas each group 3 pillars that need being developed to create National Cyber Sovereignty.

These 18 pillars are the backbone of Thales’ National Cyber Sovereignty Index.

A Nation’s government can easily perform a preliminary assessment of their country’s state of play for themselves:

- **Red**: High-priority – Pillars are absent or only poorly developed.
- **Orange**: Medium priority – Pillars are in place but require to be enhanced.
- **Green**: Low priority – Pillars are in place and functional.
A Nation’s roadmap towards Cyber Sovereignty is driven by its National Cyber Strategy (NCS).

The NCS defines long-term goals and the pieces of legislation required to that end. It exposes the pillars that need to be built or enhanced to that end and the subsequent national roadmap.

The National Cyber Agency (NCA) will then implement that roadmap in the legislative context set to that end. Each year, projects will be run by the NCA with the resources allocated for the occasion.

So goals define the possible routes towards Cyber Sovereignty. For instance, if the goal is to protect the secrecy of governmental communications, then secured telephones have to be procured. In turn, this entails the need for trusted suppliers and duly certified or qualified hardware and software. Sovereign crypto mechanisms are also required, which in turn also means that trusted national research laboratories, equipped with highly trained scientists, develop the expected algorithms.
5. Working with Thales

Thales helps Governments to assess, to set-up and to enhance cyber sovereignty and is well-known for being a highly-trusted partner of Governments and Critical Infrastructure Operators around the World. There are good reasons for this, which have long been positively evaluated by our many customers worldwide. Against each of the six areas of the NCSI, clients say they are:

1. National Cyber Strategy:
   - Nonalignment & Objectivity;
   - Partner of several National Cyber Agencies, the European Union and others;
   - A vast multi-domain, multi-technology experience;
   - An in-depth practice of cyber resilience engineering frameworks;
   - The Co-construction + Build-to-Goals approach of all our projects;
   - Our proactive participation in International Cyber Governance;

2. National Education & Training Strategy:
   - The CyberTrain Framework™ for setting-up Cyber Academies;
   - Hands-on approach to Education & Training;
   - CyberRange technology in support of technical training and cyber exercises;

3. National Research & Technology Strategy:
   - Thales’ R&T programme that is considered as an example in the Industry;
   - 2500 researchers working across TRL1 to TRL6 only, and a Nobel Prize;
   - Multiple research chairs & sustained academic partnerships already;

4. Corporate Cyber Maturity Enhancement:
   - Support to International Projects (Galileo, SESAR, ...);
   - Assessment, selection and implementation of best-fit, good cyber practices;

5. Sovereign Solutions & Technologies:
   - Qualified & certified open source solutions policy;
   - Supply of trusted customisable solutions in support of Cyber Sovereignty;
   - Sovereign solutions qualified by your National Cyber Agency;

6. Governmental Capabilities:
   - Experienced with all sovereign cyber capabilities;
   - Sound circumstance-driven methodological approaches for implementation.