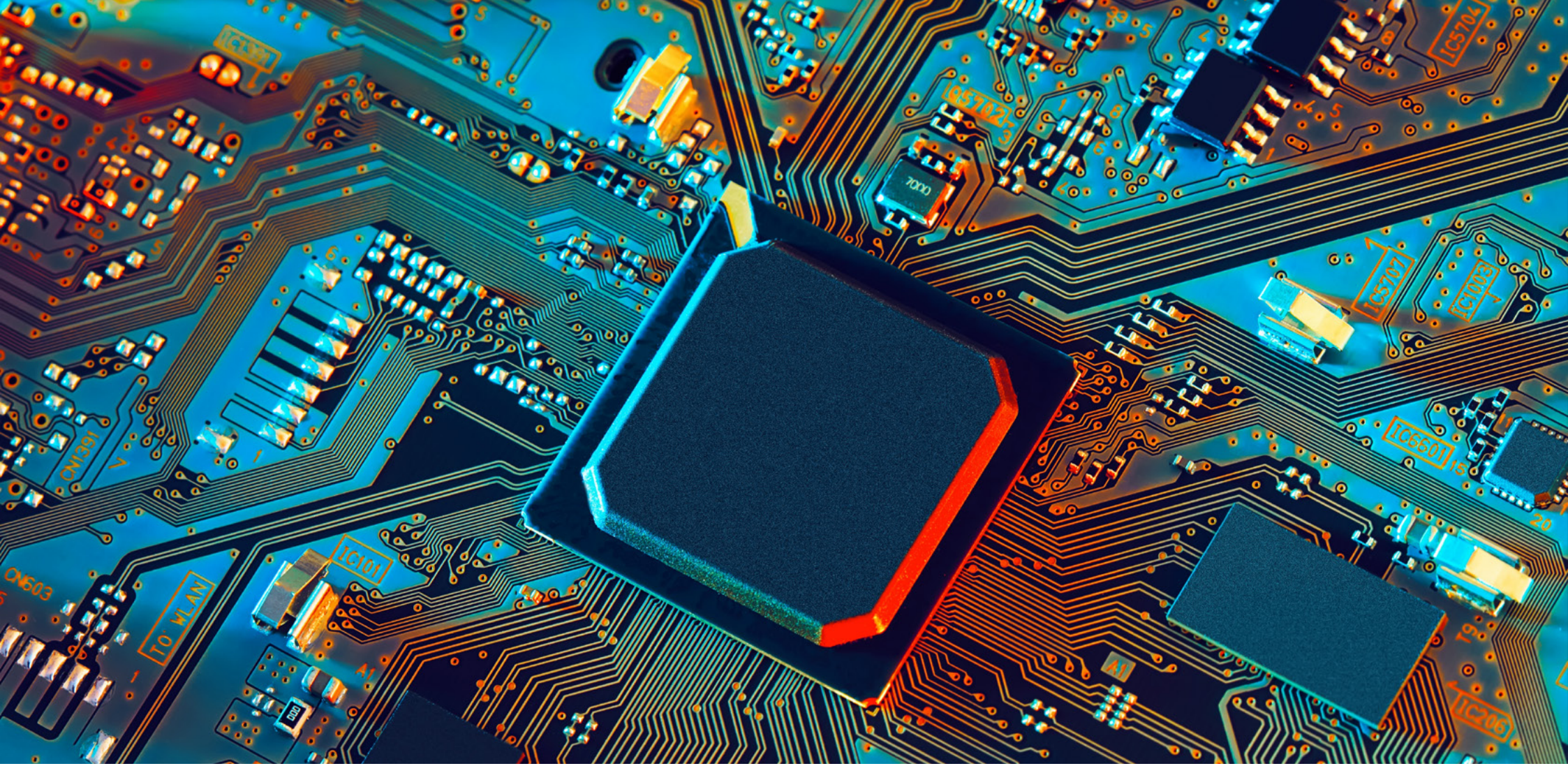

Summary

Improve the connection

Evaluation of the international cybersecurity policy of the Dutch Ministry of Foreign Affairs

Background and importance

Below is a summary of the key findings and recommendations of the evaluation of the Dutch Ministry of Foreign Affairs (MFA)'s international cybersecurity policy, conducted by the Policy and Operations Evaluation Department (IOB) within the ministry.

Increasing threats

During the evaluation period (2015–2021), cyber threats increased worldwide. Digital attacks for which states or other actors are responsible are now a daily occurrence in the Netherlands and abroad. Although these attacks do not always attract publicity, their consequences are increasingly noticeable for governments, companies and citizens. In addition, a dichotomy has emerged internationally between predominantly Western countries (including the Netherlands) that generally strive for a globally open, free and secure internet, and countries such as Russia and China that wish to curtail citizens' free access to the internet (see chapter 1). The hardened geopolitical situation and the increased number of incidents make it difficult to reach global agreement on norms for state behaviour and the application of international law in cyberspace.

The Dutch international cybersecurity policy

The international cybersecurity policy of the MFA is aimed at preventing and mitigating cyber threats and attacks by states and state-affiliated actors directed against targets in other states. The Taskforce Cyber (TFC) was set up within the MFA in 2015, with the purpose of implementing this policy. Its work can be roughly summarised as 1) diplomatic response and coordination in the event of cyberattacks and related incidents; 2) diplomatic engagement to promote the international rule of law in cyberspace; and 3) financial assistance for cybersecurity capacity building in other countries.

Importance of the evaluation

The growing number of cyber threats directed towards the Netherlands has resulted in increasing public and political awareness of challenges in the cyber domain, making the TFC's work even more urgent. However, as a relatively young policy area, the international cybersecurity policy of the MFA has never been evaluated up to now. This first evaluation shows that since 2015, the TFC has often done good work and achieved things, but there are also challenges and areas for improvement. Although the evaluation focused on MFA's international cybersecurity policy, during the study it became clear that some of the key challenges – and solutions – are government-wide. The start of a new cabinet makes this a good time to look ahead and sharpen international cybersecurity policy, for which this evaluation makes recommendations.

The study

The evaluation investigated what did and did not go well in the policy's design and implementation, and which recommendations follow from this. The full report (in Dutch) can be found here: www.iob-evaluatie.nl/resultaten/internationaal-cybersecuritybeleid. It is based on interviews with 95 stakeholders and experts, the findings from a survey amongst 73 stakeholders and experts, an analysis of internal and external documents and a literature review.

Main findings and recommendations

Interdepartmental cooperation: part of the problem and of the solution

Several ministries are involved in aspects of the international cybersecurity policy. During the evaluation period (2015–2021), a number of interdepartmental policy documents related to international cybersecurity policy were drafted and interdepartmental cooperation improved. Nevertheless, the evaluation revealed there are still issues with departmental alignment and cooperation in relation to international (as well as national) cybersecurity policy. For example, ministries still too often work independently of each other, are not always sufficiently aware of each other's work, do not always make sufficient use of the expertise of other departments and do not always cooperate sufficiently with each other. As a result, threats and opportunities are missed, work is inefficient, and policy is not always consistent. One of the main causes of the cooperation problems is the departmental compartmentalisation of cybersecurity policy in the Netherlands, which is reflected in the facts that departments each set their own priorities, there is no national supra-departmental cybersecurity strategy and there is no centralised control of cybersecurity policy that could formulate such a strategy and set priorities.

Recommendations

For the Dutch cabinet:

1. **Investigate the best form for supra-departmental oversight of cybersecurity issues, and create this.**

Supra-departmental oversight is needed to establish mandates and tasks relating to new issues and policy themes, to weigh up the various interests of the departments involved, to promote coordination between these departments and to draw up, monitor and if necessary adjust a supra-departmental cybersecurity strategy.

There are several options for achieving this, each accompanied by its own drawbacks (see chapter 2). It needs to be investigated which option is most suitable to achieve the policy objectives and provide a solution for the problems identified.

2. **Create a supra-departmental cybersecurity strategy.**

The supra-departmental strategy presents a cabinet vision of the path the Netherlands wishes to follow in relation to cybersecurity-related issues. It should not be a summary of what the departments already do or intend to do, like the current Netherlands Cybersecurity Agenda (NCSA). Instead, it should establish links between the various policy themes by setting priorities, resolving any conflicting interests, introducing concrete objectives and exploring how these objectives can be achieved.

International cybersecurity policy within the MFA

The evaluation showed that the TFC is doing much good work. As discussed in chapters 4 and 5, the Netherlands has a strong international profile and within international forums has helped shape important instruments such as the EU cyber diplomacy toolbox and cyber sanctions regime. The creation of a network of cyber diplomats at a number of Dutch embassies was also a strong move.

However, there are also a number of issues that can be improved. For example, there is limited cyber expertise within MFA, and the available capacity within the TFC (as in other parts of government dealing with cybersecurity policy) is limited considering the increase in cyber incidents and global challenges and the time required to coordinate departments. In addition, within MFA there is no unambiguous and up-to-date strategy, nor are there frameworks delimiting which themes fall within the TFC's remit. This makes it more difficult to prioritise properly, causes some strategic issues to remain unaddressed and adds to the already high workload.

Recommendations

For the MFA:

3. **As part of or following from a new supra-departmental cybersecurity strategy, also create a new strategy for MFA's international cybersecurity policy. Ensure that:**

    a. Clear definitions and frameworks are included so that it is clear what does or does not fall under the responsibility of the TFC; and it is set out what the short-, medium- and long-term objectives are, how they link up and how they are expected to be achieved (see chapter 3).
    b. A response is given to strategic issues that arise as a result of increasing cyber threats, global disagreements, emerging technologies and new policy themes. Examples of issues to address are how the Netherlands and like-minded countries can best involve the so-called 'swing states', how capacity building can best be deployed and the tenability of the Dutch rejection of an international cyber treaty (see chapter 4).
    c. In light of the rapid developments in the cyber domain, time and capacity are factored in to ensure regular strategic reflection and scenario thinking about various possible future developments and threats.
    d. When drawing up the strategy, there is collaboration with other ministries and stakeholders from the business community and knowledge institutions.

4. **Investigate how the work of the TFC can be prioritised more sharply in order to reduce the workload.**

Use the new strategy to make explicit which activities and dossiers justify which efforts of the TFC and – in consultation with other departments and directorates within MFA – which dossiers and activities it might be better to drop or reallocate.

5. **Ensure that MFA has sufficient capacity to carry out important tasks within the international cybersecurity policy. Three issues should be considered in relation to this:**

    a. **Expand the TFC workforce.**
    In light of the increasing threats and incidents, global disagreements, emerging themes and technologies, strategic issues and the resulting (interdepartmental) challenges, sharper prioritisation will not in itself be sufficient and so the TFC needs additional capacity.

    b. **Consider ways in which knowledge and expertise on cybersecurity-related topics can be acquired and maintained.**
    These could include giving greater encouragement to employees with experience in cybersecurity-related topics to, when they move on within the ministerial rotation system, take on a new role relevant to the theme. The *Werkgroep Vervullen Vacatures* (Working Group on Filling Vacancies) initiatives to improve staff inflow and outflow at MFA could be used for this purpose. In addition, MFA could proactively address knowledge gaps by acquiring knowledge from outside the ministry through more public-private collaboration.

    c. **Invest in secure and effective means of communication.**
    In addition to investing in people and knowledge, it is also important for MFA to provide the TFC and the missions relevant to them with properly functioning and secure means of communication, so that confidential information can be shared with for example other departments, international partners and cyber diplomats (see chapter 5).

Improve the connection | IOB Evaluation | Improve the connection | IOB Evaluation | Improve the connection | IOB Evaluation | Improve the connection | IOB Evaluation | Improve the connection | IOB Evaluation | Improve the connection

Published by: Dutch Ministry of Foreign Affairs
Policy and Operations Evaluation Department (IOB)
PO Box 20061 | 2500 EB Den Haag

english.iob-evaluatie.nl
www.twitter.com/IOBevaluatie

ISBN: 978-90-5146-068-1

Design: Today | Utrecht

Photo cover: Shutterstock