Ministry of Foreign Affairs

International Cyber Strategy 2023 – 2028

Decisive Diplomacy in the Digital Domain

Contents

Summary

The Netherlands aims to contribute to an open, free and secure cyber domain. That aim, incorporated in the first International Cyber Strategy in 2017[1] and the 2022 Netherlands Cybersecurity Strategy (NLCS)[2], remains current. Since 2017, however, the geopolitical and technological context in which that aim is being pursued has changed dramatically.

The Russian war against Ukraine means that Europe is once again facing a major conventional conflict, as a result of which Russia has placed itself outside the international order. The effects of China's assertiveness as an economic and military power are also being felt. The geopolitical tensions generated by these developments have a direct impact on the digital environment. There, too, fundamentally opposing visions prevail, putting openness, freedom and security under ever-increasing pressure.

Because the digital environment has now become an integral part of our society, partly as a result of rapid technological advancements, more effective action is needed to protect our interests. The constant cyberattacks directed at our government bodies, businesses and citizens not only inflict enormous immediate damage; they also threaten our strategic national interests.

Parallel to this, the gap between digitalised and less digitalised countries is becoming increasingly evident. Many countries are unable to make cybersecurity an integral part of their digitalisation processes and policy. That makes them vulnerable to cybercriminals and state actors conducting malicious cyber operations. These developments also mean that people in those countries are more likely to be targeted by human rights violations online. Finally, the lack of cybersecurity slows down socioeconomic development.

With this interministerial international cyber strategy (ICS), the Dutch government sets out how it will respond to these international developments over the coming years by strengthening our efforts in the EU and NATO, and by expanding existing partnerships and creating new ones. Our commitment can be summarised as follows.

To counter the cyber threat posed by states and criminals, the Netherlands will deploy the means at its disposal in a more proactive, more integrated and more strategic manner, where possible in collaboration with EU partners and NATO Allies, thus aiming for maximum effectiveness in addressing state and non-state threats. These means include diplomacy, sanctions, economic leverage, intelligence-driven investigations, military and judicial competencies, and collaboration with the private sector. At the same time, these individual instruments will be strengthened.

To strengthen democratic and human rights principles online, the Netherlands will, with increased commitment and in a broad coalition of countries, researchers, academia, businesses and civil society organisations, detail how internationally recognised principles should be applied in cyberspace to promote global cybersecurity. Cybersecurity and human rights are complementary and mutually reinforcing. Individual safety is a core component of cybersecurity, and an open, free and secure internet is a crucial starting point in promoting human rights online. In addition, the Netherlands urges states and businesses to counter any violation of human rights online, whether deliberate or unintentional. The Netherlands is also committed to safeguarding human rights and democratic principles when developing standards for new technologies and online services.

To maintain a global open, free and secure internet, the Netherlands will protect the public core – in other words the technical layer – of the internet, partly in order to prevent fragmentation. Fragmentation on the internet is in a certain sense already a fact. For the technical layer of the internet, however, it should be prevented at all times. The Netherlands will also promote the involvement of emerging countries in internet governance and share expertise to further strengthen their cyber capabilities so that they too can reap the benefits of a secure digital environment.

1 Parliamentary Paper 26 643, no. 447.
2 Netherlands Cybersecurity Strategy 2022–2028, October 2022.

Introduction

Structure of the International Cyber Strategy

The ICS sets out what the various ministries will be doing in the realm of international cyber policy over the next five years (2023-2028). An analysis of the main developments in cyberspace can be found in section 1 (Global developments in cyberspace). Section 2 (Objectives) explains how those developments translate into three policy objectives and which instruments will be used to achieve those objectives. At the end of the strategy, the reader will find a non-exhaustive list of specific actions that have been identified to further define the result areas, as well as information on which ministries and agencies bear primary responsibility for performing those actions. The list builds on the action plan issued with the NLCS[3] and will be updated regularly over the next few years.

Conditions for the effective implementation of international cyber policy

In the competition for strategic political and economic interests that is playing out in cyberspace, the Netherlands can only operate effectively – in international coalitions – if our international efforts in the cyber domain are integrated in a broader foreign policy context. Boosting our own cybersecurity and that of third countries is not merely a technical matter that can be seen in isolation. The challenge is to link international cyber policy to relevant foreign policy issues such as security (including economic security), human rights, the rule of law and multilateralism, as well as to the broader commitment within the EU, NATO, the OSCE and the UN. In that light, cyber issues should become a more routine part of diplomatic work, such as formal political or security consultations with third countries, and should be raised at meetings of the various configurations of the Council of the European Union, such as the Foreign Affairs Council (including Defence and Development Cooperation) and the Competitiveness Council.

Similarly, a link needs to be established between international cyber policy and the foreign trade and development cooperation agenda. Cybersecurity, in the sense of protecting the confidentiality, integrity and availability of information systems, is one of the prerequisites for a stable society, for sustainable and forward-looking economic development and for user safety in emerging countries. What's more, inadequate cybersecurity elsewhere can affect cybersecurity close to home. As part of our commitment to increasing digitalisation under the foreign trade and development agenda, it is necessary to address maintenance and security of IT solutions from the outset. Helping to close the gap with less digitalised countries is a key concern in this regard.

To be able to respond to relevant cyber developments in third countries, the cyber expertise and capabilities of Dutch missions abroad must be enhanced. The amendment submitted by MP Agnes Mulder et al. enabled the Ministry of Foreign Affairs to augment the number of embassy-based cyber diplomats considerably.[4] As a result, a growing number of positions at 34 embassies and permanent missions and representations now include a significant cyber component. That investment is bearing fruit. For instance, the Netherlands is engaged in dialogue with a growing number of countries and is regularly asked to share knowledge and expertise in multilateral working groups and at cyber conferences. The Netherlands has raised its profile as a relevant cyber actor in many countries by deploying cyber diplomats as well as the Dutch Ambassador-at-Large for Security Policy and Cyber. This deployment also leads to more intensive local cooperation with attachés from, for example, the Ministries of Economic Affairs and Climate Policy, Defence, the Interior and Kingdom Relations, and Justice and Security. The need for further development of cyber knowledge and expertise also applies to the ministries in The Hague. We will maintain as much existing cyber knowledge within ministries and governmental organisations as we can and bring in external expertise where necessary.

3 https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy---action-plan.

4 https://www.tweedekamer.nl/kamerstukken/amendementen/detail?id=2021Z20724&did=2021D44130 (in Dutch).

Global developments in cyberspace

Digitalisation has been the engine driving our development over the past few decades. It has enabled many countries to develop their economies and sectors such as healthcare, transport and energy. We will continue to reap the benefits of digitalisation in the future, especially with the emergence of new digital technologies such as artificial intelligence (AI) and quantum technology. Digitalisation has provided increasing global interconnectedness and has lowered barriers to relations between countries. In times of geopolitical stability, the risks associated with intensified interconnection are manageable, but in times of geopolitical turmoil, this digital interdependence can lead to major challenges. Moreover, exponential digitalisation has generated greater opportunities for malicious actors and increased the overall attack surface, and this threat will only grow in the future as digital technologies continue to develop.

The geopolitical dynamic that is unfolding in the physical world also translates to the digital environment. Our national security, our earning potential and the safe online environment for the individual are threatened on a daily basis by state and criminal actors. Just like the physical world, the digital world is now an arena for strategic competition, in which conflicting interests and values increasingly lead to confrontation. In cyberspace, this competition is expressed through cyber operations – espionage, sabotage and the dissemination of disinformation.

This dynamic is reinforced by rapid technological developments. Due to the greater accessibility and relatively low cost of cyber tools and the application of new digital technologies in cyber operations, we are witnessing a proliferation of threats by states and cybercriminals. New and cheaper cyber resources are not only used for foreign cyber operations and espionage; they also make it easier for actors to hack, threaten and persecute their own citizens (lawyers, politicians, human rights defenders, journalists) online. The false dichotomy between cybersecurity and human rights is also trotted out more often. For instance, internet shutdowns are often justified as issues of national security.

The emergence and further development of technologies also raises questions about internet governance and the development of standards for new technologies. For a long time, discussions on internet governance and technical standards for new technologies involved meaningful engagement of both state and non-state stakeholders. In the current geopolitical climate, however, that multi-stakeholder model is under pressure. Various states are attempting to multilateralise technical discussions, thus putting engagement of civil society organisations, the private sector, academics and the tech community under pressure. This also has implications for the internet governance model.

In order to address these broad and complex challenges effectively and comprehensively, an assertive European Union is essential. Europe has already taken important steps in terms of legislation to provide better protection for businesses and the public against state and non-state cyber threats, for example through the Network and Information Security Directive (NIS2) and the Digital Services Act (DSA). At the same time, it is worth asking whether the Union should not be even better equipped in the field of foreign policy in order to play an effective part in the strategic competition that is becoming more acute in the digital environment. To do so, it would seem necessary to reinforce the shared sense of urgency among member states and EU institutions about the strategic cyber threat posed by a number of states. Technological developments should also be viewed more regularly through a geopolitical lens by strengthening the link between internal legislative programmes and Europe's external cyber policy.

Our multipolar world also means that merely maintaining existing coalitions and partnerships – such as the EU, NATO and the transatlantic partnership – is no longer enough to be able to defend our interests effectively in cyberspace. Cybersecurity and the configuration of cyberspace are, by definition, transnational issues, which means that the importance of new partnerships is growing. It serves the Netherlands' strategic interests if countries with which we maintain political and economic relations become more resilient to external cyber threats and are themselves better able to defend their own sovereign interests in cyberspace.

In this context, we also see that the relative influence of emerging and developing countries in multilateral cyber discussions is growing, for instance on the applicability of

international law in cyberspace and a common approach to cybercrime. In strengthening ties with new partners, it is important to strike a balance between, on the one hand, the ultimate target of an open, free and secure cyber domain and, on the other, promoting our own direct interests in a complex reality in which not all countries with whom we cooperate fully subscribe to our values and principles.

Objectives

Overall objective of Dutch international cyber policy:

The government's aim is an open, free and secure cyber domain in which states act responsibly, universal human rights and the principles of the rule of law are guaranteed, the applicability of international law is recognised and the decentralised and open nature of the internet is preserved.

Geopolitical developments are making the circumstances for the achievement of this objective highly complex. Power shifts and rising tensions in combination with rapid technological advancements are leading to a growing geopoliticisation of cyberspace. These developments translate into three high-priority challenges for the coming years:

Cyber operations that are increasingly used to pursue strategic political, economic and military goals are putting pressure on our security and prosperity

For example, political and economic espionage, disinformation and sabotage

Democratic and human rights principles online are coming under growing pressure

More and more regimes are using digital technologies to strengthen their own position and to control their citizens, civil society and opposition. Take for instance the use of surveillance technology and internet shutdowns.

Growing politicisation of international technical organisations

States are trying to increase their influence on the shaping of standards for new technologies as well as on how the internet is configured, by limiting input by the private sector, civil society organisations and academics.

On the basis of these challenges, the Dutch government has set **three objectives** for the 2023-2028 period:

1. *Combat cyber threats posed by states and criminals*
2. *Reinforce democratic and human rights principles online*
3. *Maintain a globally interconnected open, free and secure internet.*

In addition to the identified result areas and specific activities, a number of **cross-cutting policy instruments** are relevant to the pursuit of these objectives. They form a common thread that runs through our international cyber policy for the next five years:

- Expanding the role of the EU and NATO as international cyber actors;
- Using multilateralism as an instrument to achieve responsible behaviour in cyberspace;
- Strengthening existing coalitions with emerging countries and building new ones;
- Investing in intelligence capabilities;
- Actively involving the cyber community (private sector, civil society organisations and academics) in cyber issues;
- Reinforcing the diplomatic network and increasing technical and policy-related cyber knowledge.

Strategic objective 1

Combat cyber threats posed by states and criminals

Result areas

- Moving from a reactive to a proactive approach to cyber threats
- A clearer sense of the threat
- Increased clout in cyberspace
- Effective international coalitions
- Reinforcing and maintaining norms for responsible state behaviour
- Closer international cooperation against cybercrime

Analysis

In line with the geopolitical developments referred to earlier, we are now seeing that states are using cyberspace systematically and intensively to serve their own interests. Cyber operations, such as political and economic intelligence gathering, influencing and sabotage, are important instruments in this regard: they are relatively cheap and scalable with a high, often long-term yield. Cyber operations usually fall below the legal threshold of an armed conflict, but the cumulative effects of the many individual cyber operations potentially come close to the effects of an armed attack. All the more so because cyber operations are conducted in conjunction with resources that lie outside cyberspace, as occurs in hybrid campaigns. Over and above the cyber threat posed by state actors, cybercrime (possibly sponsored or facilitated by states) has grown to become a potential threat to national security.

To curb malicious state behaviour in cyberspace and reduce the risk of conflict, intensive negotiations have been conducted over the past few years, particularly within the UN, on international agreements to which states should adhere in cyberspace. In parallel, efforts have been made to agree on an international approach to cybercrime. The Netherlands has played an active role in these negotiations. In the current geopolitical climate, however, the likelihood of further consensus agreements within the UN on norms in cyberspace or on cybercrime prevention seems slim.

Russia and China, supported by a number of partners, appear to put into question the existing UN framework for responsible State behaviour in cyberspace repeatedly endorsed by all UN Member States. Within the UN they are presenting themselves as advocates of an agenda designed to restrict the scope for political dissent and freedom of speech in cyberspace. These countries also oppose the participation of non-state actors (civil society organisations, the private sector, academics and the tech community) in formal UN discussions on this topic. In addition, Russia, supported by a limited number of States, calls for a legally binding treaty on responsible state behaviour in cyberspace. The Netherlands remains committed to the consensus reached by all UN Member States that existing international law, including human rights law and international humanitarian law, applies in full to cyberspace. The Netherlands and likeminded countries are of the view that before considering the possible elaboration of legally binding obligations, UN discussions should focus on deepening common understandings of exactly how international law applies to cyberspace, with a view to reinforcing the existing normative framework and promoting its implementation. Only on the basis of such discussions can a decision be made as to whether new binding obligations may be necessary in the future.

Finally, it is important to note that because of the spectacular pace of global digitalisation and the increased cyber threats posed by state and non-state actors, interest in international cybersecurity policy is growing among UN member states in all regions. Over the next few years, emerging countries will play an increasing role in shaping the future of cyberspace. Just as on other geopolitical issues, many of these countries do not want to be forced to make a choice between the competing geopolitical blocs within the UN. Many of them also have insufficient capacity to identify and address cyber threats. This renders them vulnerable to influencing, interference and unwanted dependencies.

Challenge

The geopolitical conflict in cyberspace is coupled with the growing importance of the domain for the Netherlands' security, economy and prosperity. As a result, the cyber threat facing us has increased enormously. The strengthening of norms for responsible state behaviour in cyberspace and the formulation of responses to violations of those norms are still important in this context, but these lines of effort are not enough to ensure effective protection of our national interests.

Response

Moving from a reactive to a proactive and strategic approach to cyber threats

In response to the heightened cyber threat, we need to deploy the full range of instruments we have at our disposal to protect Dutch interests in cyberspace more proactively, more comprehensively and more strategically, wherever possible in conjunction with EU partners and NATO allies. By doing so, we will aim for maximum effectiveness in addressing state and non-state threats. Those instruments include diplomacy, sanctions, economic leverage, intelligence-driven investigations, military and judicial clout, and collaboration with the private sector.

To put the more proactive and more strategic approach we are aiming for into practice, cooperation between all national partners needs to be intensified and better targeted, both within and outside the cyber domain. This will build on the interministerial cyber response framework that has been in use since 2018, and additional models will be set up if necessary to facilitate information-sharing and decision-making. Alignment will also be sought with relevant national processes and structures, such as the government-wide response framework against state threats. In the coming years, special attention will be paid to collaboration with the private sector, which is playing an increasingly important role in countering cyber threats.

Over the past few years, the Netherlands has played a pioneering role in formulating international diplomatic responses to cyber threats, and the government aims to play a similar leading role in shaping the more proactive international approach to such threats. The Ministry of Foreign Affairs will develop this new approach further in the coming years, in close collaboration with all relevant government entities.

In addition to deploying the resources used to protect our interests in cyberspace more proactively, the individual instruments will need to be strengthened. The following paragraphs will look at this in more detail.

A clearer sense of the threat

A more strategic, proactive approach to the threat in cyberspace relies on having a clear sense of the threat. The Dutch government is therefore investing heavily in the investigative capabilities of the intelligence and security services for intelligence-oriented in-depth research.[5] In addition, in the 2022 Defence White Paper, the Ministry of Defence indicated it will share information about threats more often (including hybrid threats) if that helps allies and partners (NATO and EU) and Dutch society to protect themselves more effectively against the cyber threat.

Increased cyber power

In order to operate more assertively, the ability to project power in cyberspace is essential. The Ministry of Defence is therefore specifically increasing its cyber capabilities, partly by enhancing the exchange of information and boosting resilience, as stipulated in Article 3 of the NATO Treaty. This will help to mitigate cyber threats. Working within the relevant legal frameworks, the government will intensify existing efforts (both online and offline) for tracing, tackling, disrupting and prosecuting malicious actors and their facilitators.

On 2 December 2022, the government presented to the House of Representatives the bill concerning the temporary act pertaining to investigations by the General Intelligence and Security Service (AIVD) and the Defence Intelligence and Security Service (MIVD) of countries with an offensive cyber programme. This bill was drafted because of operational bottlenecks encountered by the AIVD and the MIVD in investigations into cyber threats posed by state actors. The bill aims to enable the services to use their powers faster and more effectively in cyberspace, while maintaining the necessary safeguards.

The Ministry of Defence is recruiting cyber experts in order to expand its offensive and defensive cyber capabilities. Its cyber readiness is also being enhanced by creating a better (cyber) intelligence position and boosting the cyber resilience of units and systems. Lastly, cooperation with international security partners will be consolidated in order to, for example, form a united front against hybrid threats. It is for that reason that the 2022 Defence White Paper is subtitled 'Investing in a robust NATO and EU'.

Effective international coalitions

Strong coalitions are essential if we are to offer robust resistance to countries with offensive cyber programmes targeting Dutch interests. Both within the EU and NATO and beyond, we are therefore improving the effectiveness of xisting instruments and developing new strategies to optimise resilience and strength.

5 See Actions and priorities for Pillar III and the Financial overview in the NLCS, October 2022.

The EU Cyber Diplomacy Toolbox – the framework of options for responding to malicious state cyber actors – needs to be better aligned with the geopolitical reality. It is currently only possible to impose sanctions on individuals and entities, while the cyber threat posed by state or state-linked actors continues to grow. So the government is calling for the EU cyber sanctions regime to be deployed more often and for harsher sanctions to be made possible. The system should also allow for a more country-specific use of cyber sanction tools.

Within the EU, it is also important to seek a connection with other instruments (such as the EU Hybrid Toolbox and the Foreign Information Manipulation and Interference Toolbox) that can be used to counter hybrid threats posed by state actors. The various toolboxes are independent instruments, but a stronger connection makes it possible to operate more effectively and to counteract fragmentation.

Closer EU-NATO cooperation is also needed to deal with cyber threats. Here, opportunities are being sought for EU and NATO activities to be mutually reinforcing, within their respective competences and without causing unnecessary duplication. This can be done in a number of ways, such as: seeking synergy between the EU Cyber Diplomacy Toolbox and the NATO Guide on the diplomatic response to cyber incidents, organising joint cyber training exercises and engaging in practical collaboration at working level and capacity building on issues such as cybersecurity.

Finally, cooperation with countries outside the EU and NATO will be explored and intensified further. Countries such as Japan, South Korea, Australia and Singapore are facing similar cyber threats as the Netherlands and are also investing in their capacity to address these threats.

Many other countries lack the necessary capacity to identify or address cyber threats posed by states and cybercriminals. The government is therefore strengthening cooperation with partners in the Western Balkans – partly because of the continuing threat those countries face from Russia – and also in southern Africa and the Indo-Pacific. Many countries in those regions are undergoing rapid development, but in doing so, they are also becoming an easy target for cyber-attacks and cybercrime. These countries also play an increasingly prominent role in the geostrategic competition that is playing out in cyberspace. Dutch involvement is helping those countries to boost their cybersecurity as well as attempting to increase their involvement in multilateral discussions on responsible state behaviour and cybercrime prevention. We are also seeking alignment with the Dutch and European Indo-Pacific Strategies, the Africa Strategy and the EU's Global Gateway programme. The UN provides an important platform for establishing new contacts. Bilateral and regional cyber consultations are also being used to explore ways in which the Netherlands can cooperate further with these countries, on the basis of shared interests.

Reinforcing norms for responsible state behaviour

As a digitalised nation with an open economy, the Netherlands benefits greatly from maintaining the international legal order and multilateral agreements in the digital domain. What is more, multilateral agreements serve as a starting point for holding state actors to account for malicious behaviour. That is why in the coming years the Netherlands will continue to contribute actively to the consolidation and further development of the normative framework for responsible state behaviour that UN member states developed on the basis of consensus agreements. The normative framework includes 11 non-binding norms of conduct, practical confidence-building measures to prevent escalation of cyber incidents, and the recognition that international law applies in cyberspace. The government is also prioritising the protection of the technical infrastructure essential to the availability or integrity of the internet and stimulation of discussions about the risks to international cybersecurity associated with new technologies such as artificial intelligence. The Netherlands is also encouraging countries to implement the UN norm to not knowingly allow their territory to be used for internationally wrongful acts using ICTs. The experience gained by the Netherlands in UN discussions about responsible state behaviour in cyberspace is also relevant to discussions on new, related policy issues on which multilateral agreements are needed, such as the space domain and military use of AI.

Within the UN, the government is particularly committed to developing relations with emerging and developing countries. Special attention is given to major regional players. An important objective of the UN discussions is that all countries will ultimately be able to implement the agreements that have been made. To advance the further development and implementation of the normative framework, the Netherlands supports the French-Egyptian initiative for a UN Programme of Action to advance responsible state behaviour in cyberspace.

Finally, the Netherlands is working with a number of partner countries to increase the participation of women representatives in UN processes through the Women in Cyber Fellowship. Through this programme, both the number of women and the number of actively participating countries in UN negotiations have risen significantly. The government is committed to the continuation and expansion of this programme.

Closer international cooperation against cybercrime

To counterbalance the global increase in damage caused by cybercrime, the Netherlands is concentrating its efforts on a

number of avenues. Dutch diplomatic efforts in respect of cybercrime prevention are focused primarily on denying safe havens to cybercriminal groups in accordance with the UN normative framework and the Council of Europe's convention on cybercrime, the Budapest Convention. The Netherlands is also taking part in negotiations on a UN treaty on cybercrime. It is important to ensure that this treaty strengthens the international approach to combating cybercrime, but cannot be misused to restrict human rights online, such as the right to freedom of expression. Within the EU, the Netherlands is a driving force in this process. We are also assisting countries with combating cybercrime, for example by helping to draft or harmonise legislation in line with the Budapest Convention.

In combating cybercrime, from prevention and disruption to response and from investigation to prosecution, the government collaborates closely with countries within and outside the EU. This collaboration includes providing legal assistance in criminal cases. The government is also committed to enhancing the international exchange of information on evolving cybercrime threats. The government is seeking to increase international awareness and shared understanding of these threats and how to counter them in an international context, particularly with regard to ransomware. The Netherlands is an active member of the International Counter Ransomware Initiative, a US initiative in which experiences are shared between a large group of countries on, for instance, resilience, disruption of ransomware groups, public-private cooperation and diplomacy.

The government believes that the human rights dimension of the approach to cybercrime, including robust safeguards, deserves particular attention. International agreements on investigation and prosecution could potentially impact heavily on the rights of individuals and certain groups in society, such as minorities, political opponents, journalists and the LGBTIQ+ community, especially now that technological advancements are leading to an exponential growth in investigative tools that can be used for repressive purposes. Dutch expertise in this area is also shared with various countries outside the EU, such as the US, Japan and Canada.

Commitment to increasing the EU's cyber resilience

The government makes extensive use of the opportunities offered by cooperation within the European Union to increase cyber resilience at EU level. The Netherlands is taking a pro-active role in stimulating cooperation between EU member states, thereby contributing to a cyber-resilient Union. Cyber risks of a transnational nature are thus being addressed, and a coordinated response is being mounted to address major cyber incidents and crises within and outside the EU.

In the EU context, the government will therefore continue to work actively towards sound agreements and to contribute to EU proposals and legislation designed to increase cyber resilience. The Netherlands also plays an active role in EU-wide crisis training exercises. The Netherlands Cybersecurity Strategy 2022-2028 looks in more detail at various important EU initiatives to which the government contributes for the purpose of increasing cyber resilience, such as the Network and Information Security Directive (NIS2) and the recently proposed Cyber Resilience Act.

Strategic objective 2

Strengthening democratic and human rights principles online

Result areas

- Strategic coalitions for the recognition and application of international law and human rights online
- Encouraging states and businesses to combat online human rights violations
- Safeguarding human rights and democratic principles in standards for new technologies

Analysis

In the 12 years that the Freedom House organisation has been monitoring internet freedom worldwide, that freedom has been drastically curtailed. For example, the number of internet shutdowns by governments has risen in recent years.[6] In a growing number of countries, access to the internet – or specific internet services, such as X (formally Twitter) – has been denied to users in times of political unrest or crisis, often with the aim of blocking communications or preventing information about the blocked area reaching the outside world. The Dutch government believes that access to online media and services forms an essential part of media freedom and freedom of expression. It is disturbing that these shutdowns frequently go hand in hand with other human rights violations; a recent example was the increase in police violence against protestors after the internet shutdown in Belarus. The UN reported that in Myanmar, too, restricted internet access was used to conceal human rights violations.[7] Without the internet, journalists, human rights defenders and humanitarian organisations are prevented from gathering evidence of and reporting on such situations.

Internet content

Besides restricting internet access, governments in many countries also target internet content in order to silence dissident or marginalised voices. For example, legislation aimed at 'cybersecurity' is often misused to ban online criticism of the government in a broad sense, or there may be strict content moderation regulations in place whereby authorities order certain unwelcome posts to be removed from internet platforms as a condition for their access to national networks. Countering disinformation and hate speech is used by many states as a pretext for censorship.[8]

On the other hand, content is used as a tool to influence discussions in the online public domain. Disinformation is used to justify the war in Ukraine. Hate speech and extremism are permitted in order to, for example, intimidate women (members of parliament in particular), political opponents or marginalised groups to such an extent that they withdraw from public debate. In the coming years, the international community will face the challenge of finding a balance between countering this kind of damaging disinformation, hate speech and propaganda and, at the same time, ensuring a free and pluralistic online media landscape.

Technological surveillance

Far-reaching digital advancements, for example in artificial intelligence, are enhancing the effectiveness of existing technologies and applications. This includes applications that enable digital surveillance. Examples of these applications are facial recognition technology, big data analysis and software for hacking into devices such as phones. This technology can be used for legitimate purposes. It could be a crucial tool in, for example, crime prevention. But the same technology can also be misused to gain political control or to suppress opposition, in violation of universal human rights. Sadly, there are countless examples from around the world in which such technology has been used unlawfully against lawyers, politicians, human rights defenders, diplomats or journalists.

6 On 1 March 2023, Access Now published a report showing that 2022 had seen the highest number of shutdowns ever: 187, in 35 different countries. Access Now, #KeepItOn report 2022:https://www.accessnow.org/internet-shutdowns-2022/.

7 UN Press release of 7 June 2022, 'Myanmar: UN experts condemn military's "digital dictatorship"' https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship.

8 See the report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: 'Disinformation and freedom of opinion and expression'.

Development of new digital technology

Technical standards play a key role in the further development of the internet and new digital technologies. Standards provide detailed specifications about how a technology should work, so that it satisfies certain quality requirements and is interoperable with other products, even those produced by a different manufacturer. This is also true for applications that can be used to control or oppress citizens. In recent years, we have seen a surge in the influence of non-Western countries, including China, on the development of standards for new digital technologies such as 5G, quantum technology, big data and AI. The increased focus on cybersecurity and the demand for innovative solutions mean that international standardisation organisations increasingly find themselves working on standards that could potentially affect application of human rights. This could lead to new products which, on the basis of technical standards for quantum technology or AI, for instance, would enable the perpetration of human rights violations.

Challenge

Although there are plenty of states that use new digital technology legitimately, there is also evidence of a shift in the other direction. Because of new legislation, censorship, disinformation, shutdowns and surveillance, for example, online human rights violations are on the rise. As a result, the internet is increasingly being used as an instrument for oppression rather than a means of promoting security, development and prosperity. Although such violations are frequently raised in the multilateral debate, countries guilty of committing them often hide behind the argument that there are not yet any international agreements on the application of human rights online.

Technologies such as facial recognition are also valuable as consumer applications, but these too can be used to violate human rights. The use of standards set by a multilateral organisation validates the application of these technologies and facilitates international trade in products that use them. This increases the likelihood of human rights violations. Because of this development, standardisation of new digital technologies can no longer be viewed solely from a technical perspective.

Response

Strategic coalitions for the recognition and application of international law and human rights online

For the Dutch government, it is crystal clear: international law and human rights apply online as well as offline. This is also recognised by the UN.[9] Wherever possible, principles that we have enshrined in international treaties concerning good governance, the rule of law and human rights should be translated directly to the digital environment. In some cases, this translation is not immediately possible, for example if the technology is new and the human rights risks have not yet been identified. In such cases, we work in a broad coalition of countries, researchers, businesses and civil society organisations to determine how internationally recognised principles should be applied.

In this spirit, the Dutch government will work in the coming years to expand the Freedom Online Coalition (FOC), which the Netherlands set up in 2011. Currently, 38 countries are members of this coalition. The FOC has established itself as a leading group that campaigns for the recognition of human rights online and issues joint statements on this subject in relation to areas in which no international consensus has yet been reached. Prime examples of these are joint statements regarding measures to counter the spread of disinformation online,[10] artificial intelligence and human rights,[11] digital inclusion[12] and the 'Guiding Principles on Government Use of Surveillance Technologies'.[13] By means of statements and internal coordination, FOC members endeavour to achieve the best possible outcome in UN negotiations.

The FOC is already a diverse diplomatic coalition comprising countries from every continent, but the Netherlands is seeking further expansion. To increase the legitimacy of the FOC and to demonstrate that these issues are a concern for a wide-ranging group of countries, it is especially important to encourage more emerging countries to become members of the coalition. As well as diplomatic coordination, the coalition also offers the possibility of sharing knowledge and expertise on these issues in order to increase capacity in public services. The government is therefore committed to an expansion of the FOC by at least 10 members in the next five years, with the emphasis on emerging countries.

9 See the final UN report (A-AC.290-2021-CRP.2) from 2021 which states: 'States reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.' Final report A-AC.290-2021-CRP.2.docx (un-arm.org). Also UN human rights resolution A/HRC/20/L.13 from 2012: 'The promotion, protection and enjoyment of human rights on the Internet'. [

10 Freedom Online Coalition, November 2020, Joint Statement on Spread of Disinformation Online: https://freedomonlinecoalition.com/wp-content/uploads/2022/03/FOC-Joint-Statement-on-Spread-of-Disinformation-Online.pdf.

11 Freedom Online Coalition, November 2020, Joint Statement on Artificial Intelligence and Human Rights https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-Artificial-Intelligence-and-Human-Rights.pdf.

12 Freedom Online Coalition, February 2020, Joint Statement on Digital Inclusion. https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-Digital-Inclusion.pdf

13 Freedom Online Coalition, March 2023, Guiding principles on Government Use of Surveillance Technologies https://freedomonlinecoalition.com/wp-content/uploads/2023/03/FOC_Guiding_Principles_on_Government_Use_of_Surveillance_Technologies.pdf.

Furthermore, the government will stress the importance of a closer relationship between the European Union and the Freedom Online Coalition.

At the same time, the government will work to ensure that other diplomatic coalitions on issues relevant to cyberspace work closely with the FOC. In this respect, the government is focusing on the issues of democracy (International IDEA – Institute for Democracy and Electoral Assistance), media freedom (Media Freedom Coalition) and LGBTIQ+ rights (Equal Rights Coalition).

Encouraging states and businesses to combat online human rights violations

As well as communicating how international law and human rights apply online, it is important to effectively address any violations. Over the coming years, the government will continue to play a proactive role in addressing online human rights violations or violations of other international treaties in the digital environment. This can be done by means of bilateral consultations, either public and behind closed doors, or through the coalitions referred to above. The recently published FOC joint statement on internet shutdowns in Iran[14] following the women's rights protests is a good example that should be repeated in the coming years.

The unlawful use of technology by some states for digital surveillance (such as facial recognition technology, big data analysis or intrusion software) is a cause for concern. While the Netherlands recognises that lawful use of such technology is possible, it stresses the importance of an accompanying transparent legal framework. As a result, if and when the Netherlands uses digtial technology for investigation or for resons of national security. The Netherlands uses digital technology for investigation or for reasons of national security, in accordance with legislation and after careful consideration, within parameters defined by the principles of human rights and the rule of law. In the field of investigation, there is a requirement for suppliers of intrusion software to be screened by the AIVD; in addition, they are not permitted to sell any products to dubious regimes. The government will actively promote this example of responsible procurement in the coming years as well and will continue to advocate that the frameworks of international law also apply to cyber assets.[15] On the basis of these parameters, the government will continue to use diplomacy to call the countries that abuse these technologies to account, wherever possible in an EU context.

When addressing online disinformation and hate speech, it is important to find the balance between countering state-sponsored disinformation and propaganda on the one hand and continuing to work towards a free and pluralistic online media landscape on the other. The Dutch approach comprises the following elements: the protection and promotion of free media,[16] regulation of tech platforms and a targeted diplomatic response to disinformation from state actors. This combination of elements aims to ensure that governments can stop disinformation campaigns without affecting the freedom of expression of individual citizens. The government is following the advice of the Advisory Council on International Affairs (AIV) on this issue.[17] Furthermore, at the UN General Assembly, Canada and the Netherlands indicated their desire to work together on 'rules of the road' to stop disinformation. The Dutch government will use this initiative to work with an international coalition of countries on non-binding standards relating to the task of addressing online disinformation and responsible content moderation in a way that is consistent with human rights and international law.

It is not only states that have a responsibility to respect human rights online; businesses must do their part too. Thanks to their knowledge of the digital products that they themselves develop, tech companies should be in a better position to identify the risks and effects of their product in terms of human rights. Corporate responsibility is set out in, for instance, the OECD Guidelines for Multinational Enterprises[18] and the UN Guiding Principles on Business and Human Rights.[19] The government will endeavour to ensure that these guidelines are better observed by businesses and will urge that they be incorporated more frequently in EU partnerships with third countries. The government will also assist third countries in contacts with large tech companies and will raise the issue of violations in larger coalitions where necessary.

More and more businesses are using encryption as part of their online services, thus ensuring that privacy, confidenti-

14 Freedom Online Coalition, October 2022, Joint Statement on Internet Shutdowns in Iran: https://freedomonlinecoalition.com/wp-content/uploads/2022/10/FOC-Joint-Statement-on-Internet-Shutdowns-in-Iran_October-2022.pdf.

15 For example, the government recently endorsed the Freedom Online Coalition's joint statement on responsible use of surveillance technology by governments.

16 EU Media Freedom Act.

17 AIV advisory report no. 113: 'Regulating Online Content: Towards a Recalibration of the Netherlands' Internet Policy', 24 June 2020; government response, Parliamentary Paper 26643, no. 858, 6 May 2022.

18 OECD Guidelines for Multinational Enterprises.

19 Office of the UN High Commissioner for Human Rights, 'Guiding Principles on Business and Human Rights', 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

ality, and the integrity of information and stored data are better protected, thereby helping to prevent espionage and cybercrime. The flip side of this is that encryption makes legitimate access to data increasingly difficult for law enforcement and intelligence services. Consequently, encryption is the subject of much discussion, both in the UN and the EU. In a parliamentary paper[20] published previously, the government position on encryption was that it was currently not desirable to take restrictive legal measures in respect of the development, availability and use of encryption and that strong encryption should be encouraged. The Dutch government is conveying this conclusion and the underlying considerations internationally.

The EU has drawn up specific, practical principles surrounding applications of AI and internet services that respect human rights and the rule of law, in the form of legislation for online platforms (DSA) or on the responsible use of artificial intelligence (AI Act). It remains to be seen, however, how these principles are to be applied in practice, for example when it comes to regulating online content moderation based on the DSA. This applies both to the big tech companies and to the national regulatory authorities. It is for that reason that a conference will be organised for the various regulatory authorities from the EU member states, dedicated to the application of human rights in content moderation.

Finally, the government is propagating the principles of the DSA and the AI Act internationally to strengthen the 'Brussels effect'. Here, the aim is not simply to ensure that the legislation alone is embraced by the largest possible group of countries. Without institutional embedding of democracy and the rule of law, legislation regulating online platforms could be used for censorship, for example. The government will therefore urge third countries that fully or partially adopt this EU legislation to implement human rights and democratic principles as well.

Safeguarding human rights and democratic principles in the development and standardisation of new technologies

The development of new technologies cannot be viewed separately from international agreements on human rights and democracy. The identification of human rights risks in the application of new technology should therefore become a routine part of the development of new products. The Minister for Digitalisation has already taken steps recently to put this into practice in the Netherlands.[21] Over the next few years, the government will work to raise awareness of this policy outside the Netherlands and the EU, so that these human rights impact assessments become a fixed and reliable element in the development of new tech products. This International Cyber Strategy is thus building on the Value-Driven Digitalisation Work Agenda.[22]

Given that standards play a major role in bringing emerging technologies to market, the standardisation process must take account of potential risks to human rights. The government will keep a close eye on the development of new technical standards, focusing particularly on the increasing politicisation of the traditional technical standardisation organisations. We will also call attention to the applicability of the UN Guiding Principles on Business and Human Rights in standardisation processes.

It is likely that the development of new technologies, such as AI and quantum technology, alongside a wide range of new capabilities, will also generate new risks to human rights and democracy. Now that AI is being put to more specific use, knowledge of the risks is growing, but the same cannot be said yet for quantum technology. Against this backdrop, the government will commission a study on the human rights risks of new digital technology and discuss the issue with the Cybersecurity Council.

20 See Parliamentary Paper 26 643-383.
21 See Parliamentary Paper 32 761-262.
22 See Parliamentary Paper 26 643-940.

Strategic objective 3

Maintaining a worldwide open, free and secure internet

Result areas

- Protecting the public core of the internet
- Greater involvement of emerging countries in the governance and further development of the public core of the internet
- Increasing cyber capacity in emerging countries

Analysis

Neither the Dutch economy nor our society can function without a stable and secure digital infrastructure. As a globally connected network of networks, the internet forms the foundation of our digital world. The public core of the internet ensures that this global interconnectivity is established and guaranteed. This core, which is formed by a wide range of institutions, protocols and standards based on shared norms, values and goals, is the foundation that enables the sustainable development of new and innovative applications which in turn benefit global growth and prosperity.

Multistakeholder structure of the internet

Its wide scope and the diversity of applications and users make governance and development of this technical core highly complex. The process of internet governance is based on the multistakeholder model,[23] in which all stakeholders have an equal opportunity to see, discuss and decide on the development of and changes to the public core of the internet. The multistakeholder model applies primarily in the case of agreements about the internet itself, the management and issue of IP addresses and the technical standards that facilitate communication and interoperability between networks and applications. This open collaboration between stakeholders is embodied in organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C) and the Institute of Electrical and Electronics Engineers (IEEE). These organisations play an enabling role in adapting the technologies, standards and procedures that shape the public core of the internet.

The next few years will be crucial for maintaining this model. Agreements made at the World Summit on the Information Society (WSIS) in 2005 form the basis for the multistakeholder model of internet governance.[24] These agreements will be reviewed in the coming years, potentially leading to a renegotiation of the way internet governance is currently designed in the run-up to WSIS+20 in 2025.

Geopolitical battle for control of the internet

The neutral, apolitical and technical approach to the public core has been under pressure for some time.[25] States such as Russia and China advocate a shift of internet governance to multilateral organisations, such as the International Telecommunications Union (ITU) – the UN organisation for information and communications technology – and they are trying to garner as much support as possible for their cause. Interstate cooperation is the norm in the ITU, and the interests of non-state stakeholders, such as businesses, civil society organisations and the tech community, have less of a voice there.

At the same time, even within the EU, there are regular proposals for legislation that, in an attempt to bolster the single market, inadvertently threaten to undermine the multistakeholder model. For example, there are several

23 The development and application by governments, the tech community, the private sector, civil society and academics of shared principles, norms, decision-making procedures and programmes which shape the development and use of the internet as a globally interconnected network.

24 See WSIS Outcome documents - December 2005 (itu.int). Part of the agreement is the Tunis Agenda, in which internet governance is defined as a multistakeholder process. This document is also the basis for the organisation of the Internet Governance Forum, the UN platform where governments, businesses, academics and internet organisations hold annual discussions on internet governance.

25 From the moment the global impact of the internet became clear (in the 1990s), there has been discussion about the desired international structures for internet governance. For a historical outline of this discussion, see, for example, AIV advisory report no. 92 (November 2014), pp. 16 ff.

directives regulating elements of the domain name system (DNS), something that is traditionally shaped through the multistakeholder process. This legislation might inspire other countries to do the same or validate that approach, thus diminishing the importance of the multistakeholder process.

Lastly, we are seeing that political and economic sanctions (including restrictive measures that can be imposed by the EU) can affect organisations that play a role in maintaining the public core of the internet. Sanctions could thus inadvertently result in the fragmentation of or damage to the global technical infrastructure of the internet or the international system of internet governance. An example of such organisations are the regional internet registries, independent organisations that manage, among other things, the allocation and registration of addresses.

Internet fragmentation

Interference with the structure, management and administration of the internet jeopardises global interoperability. If a country or group of countries no longer recognises the authority of multistakeholder organisations or the importance of the multistakeholder model, this could lead to fragmentation of the public core. This would mean the coexistence of different internet systems (a free internet and a state-controlled internet). Such a split would significantly disrupt interstate communications such as e-mail and internet telephony and thus also trade, with potentially major and highly damaging consequences for global economic development and geopolitical stability.

Connectivity and cybersecurity in emerging countries

An important element of the discussion about internet governance is that a large part of the world is not yet actively involved in it. A significant number of countries struggle with limited or poor connectivity, which often goes hand in hand with poor cybersecurity infrastructure. Although the task of bridging the digital divide is already being addressed on a broad front, by the Netherlands, the EU and the World Bank, for example, the need for cyber resilience and responsible governance is not always factored into digitalisation processes. This means that in the majority of countries worldwide, the digital infrastructure, IT systems and software used are insecure, with major repercussions for data and network security and the safety of end users. This has implications locally and internationally, as a network is only as strong as its weakest link, allowing local security vulnerabilities to be exploited for attacks in other countries.

Challenge

The way the internet has been shaped and managed up to now will be evaluated in the coming years. Major changes in the governance model may result in fragmentation of the internet with potentially serious geopolitical and socioeconomic consequences. In order to keep the internet open, free and secure, non-state stakeholders such as the private sector, academics, civil society organisations and the tech community must be more actively involved in the discussions on internet governance. Also, many emerging countries are not yet participating actively in these discussions. This seems to be because many of them have their hands full with more operational challenges of digitalisation and cybersecurity, which means they are not (yet) actively engaging in international discussions on internet governance.

Response

Protecting the public core of the internet

The government believes that maintaining the integrity of the public core of the internet is key to preventing fragmentation. As the Netherlands Scientific Council for Government Policy (WRR) concluded in a 2015 report,[26] the public core must be safeguarded from improper interventions by states and other parties that cause harm and erode trust in the internet. This integrity is best preserved by protecting and strengthening the multistakeholder model of internet governance.

Protection of the public core has therefore been high on the Dutch agenda since 2015. Internet governance is the responsibility of the Ministry of Economic Affairs and Climate Policy, which represents the Netherlands in ICANN and the Internet Governance Forum. The government remains committed to increasing connectivity for all countries through organisations and partnerships,[27] improving legislation and governance, and opposing politicisation of the public core, in order to prevent fragmentation of the internet. For example, we are calling for UN recognition of the non-political nature of the public core, and we are working with internet governance forums to strengthen and ensure its independence.

Over the next few years, the government will take a leading role in multilateral negotiations (such as the Global Digital Compact and the UN's WSIS+20 review) in order to enshrine both the public/technical core of the internet and the necessary application of the multistakeholder model in new multilateral agreements.

26 'The Public Core of the Internet: an International Agenda for Internet Governance' | Report | The Netherlands Scientific Council for Government Policy (wrr.nl).

27 Such as the EU Global Gateway, ITU Development and Digital4Development hub.

In addition to protecting the multistakeholder model, the government will also commission a study into the risks of internet fragmentation, focusing on the political and technical dependencies as well as the economic implications of fragmentation. The aim of the study is not only to identify the risks for the Netherlands, but also to provide insight for third countries (within and outside the EU) into the potential consequences and to bring this to the attention of the Internet Governance Forum and other multilateral forums.

Finally, the government will urge that organisations that play an important role in the functioning of the public core of the internet should remain unaffected by restrictive measures such as sanctions. The government will be pushing for that discussion first within the EU and later within other coalitions. If organisations such as regional internet registries are affected by sanctions imposed by the EU or another body, this plays into the hands of countries who argue that the West uses sanctions to politicise the debate about how the internet works.

Greater involvement of emerging countries in internet governance

With the growing importance of the internet and digitalisation in emerging countries, those countries are also taking a more active role in the discussion on governance of the public core. While emerging countries do not always share our views on human rights online, the general principles surrounding the technical governance of the internet and the application of international law online are generally recognised.[28] For instance, a great many emerging countries have signed the Declaration for the Future of the Internet,[29] which underlines the importance of the principles described above. Because the relative importance of emerging countries is increasing on the international stage, the Dutch government wants to encourage, strengthen and expand the cooperation with those countries. The involvement of a larger group of countries will benefit the internationalisation process and strengthen the legitimacy of the current internet governance model.

The government is focusing in particular on the Western Balkans, Asia and Oceania in this respect, as well as countries in southern Africa. Through regional cyber dialogues in which region-specific cyber issues are discussed, courses to increase cyber resilience, and cooperation in forums such as the United Nations, the government wants to share experiences and strengthen relations with new partners. We will enter discussions on how best to jointly reinforce the general principles surrounding technical governance of the internet and the application of international law online.

Increasing cyber capacity in emerging countries

It is not enough to merely intensify diplomatic efforts to increase the involvement of emerging countries in internet governance processes. In the report referred to earlier, the WRR makes a distinction in the definition of internet security between the approach to 'national security' (in which national interests override the interests of the network) and 'network security' (which focuses on the security of the network as a whole). If the neutrality and effective functioning of the public core is to be maintained, the latter approach must be pursued.

Computer security incident response teams (CSIRTs), which many countries have established, are important partners in this respect. For that reason, the government will intensify its efforts to assist emerging countries in setting up or developing their own CSIRTs. For example, many CSIRTs often underperform because of poor knowledge, insufficient capacity and inadequate legislation. The National Cyber Security Centre (NCSC) has begun the rollout of a capacity-building project that includes the development and implementation of training courses. For the Dutch government, the NCSC is the connecting link in a network of national and international partners. In the event of a serious cyber incident with potential consequences outside the Netherlands, the NCSC acts as the country's first point of contact for EU member states.

Through cooperation with partners such as the Global Forum on Cyber Expertise (GFCE) – a global network of 180 countries, organisations and businesses – the task of boosting cyber resilience and expertise in third countries is being addressed. Launched by the Netherlands in 2015, this platform organises working groups on cybersecurity, cybercrime and the protection of critical infrastructure. The GFCE also seeks to identify the wants and needs in emerging countries and match them to the right agency to fulfil them.

Digitalisation cuts costs, creates economic opportunities and enhances the investment climate in low-, middle- and high-income countries. It ensures a better connection between people and thus presents opportunities to achieve the UN's sustainable development goals (SDGs) more quickly. Incorporating cyber resilience in project design is therefore extremely important but its implementation often proves challenging. The Dutch commitment to digitalisation is described in detail in the foreign trade and development cooperation policy document entitled 'Do what we do best'.

28 For example, the fact that the internet is organised on the basis of the multistakeholder model and that the organisations that carry out the management and administration of the internet do so in accordance with this consensus.

29 https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_2695/IP_22_2695_EN.pdf, a statement issued by the EU, the US and other countries on 28 April 2022.

In the coming years, working within the existing strategy and resources, the government will also specifically incorporate cyber resilience into the digitalisation projects being carried out under the foreign trade and development cooperation strategy, and together with likeminded countries, it will call for this to be addressed in the implementation of similar EU and UN projects.

In a EU context, the government is seeking to align with the Global Gateway strategy[30] of the European Commission and the High Representative: the new framework to strengthen connectivity between the EU and the rest of the world, in digitalisation and other fields, through large-scale investment. Digital economy packages combine investment in digital infrastructure with country-specific assistance in order to develop regulatory frameworks based on cyber-security and privacy. We are also seeking alignment with the UN Envoy on Technology's agenda, focusing on digital inclusion and sustainable access to new technologies. This will be reflected in the Global Digital Compact, which is expected to be adopted at the Summit of the Future in September 2024.

The government will adopt a demand-driven approach and, where necessary, use national expertise to, for example, bring legislation into line with the Budapest Convention (cybercrime), formulate policy to protect critical infrastructure, or assist in the translation of international law to the rule of law online. The network of cyber diplomats at the 34 embassies and permanent missions and representations plays a crucial role in connecting and maintaining these new and existing partnerships and initiatives.

30 This new EU strategy provides a stimulus for secure connections worldwide. To this end, the EU has developed an ambitious infrastructure plan that will be implemented by EU organisations and EU member states between 2021 and 2027.

Published by:

Ministry of the Interior and Kingdom Relations
P.O. Box 20061 | 2500 eb The Hague

September 2023