Norwegian Ministry
of Foreign Affairs

Strategy

International cyber strategy for Norway

2017

International cyber strategy for Norway

2017

Foreword by the Prime Minister

Cyberspace is developing rapidly. The global nature of the internet offers enormous opportunities, and cyberspace continues to increase in its importance to national economies, security, growth and development.

At the same time, our dependence on digital solutions increases our vulnerability. Cyberspace offers potential for new, serious transnational threats from both state and non-state actors. Norwegian society is dependent on secure, stable and robust digital networks, and a serious cyberattack could harm critical social infrastructure.

Broad national and international cooperation is crucial for Norway to achieve the best possible protection. There is a need for greater national coordination of digital security work, and for the promotion of Norwegian interests in ongoing international development of cyber-related practice and regulation.

Various aspects of cyberspace will demand our attention going forward. One example is the dependence of a sustainable internet on the right balance between openness, security, robustness and freedom. Norway advocates a cyberspace that promotes innovation and international trade, fosters international stability and security and safeguards democratic values and universal human rights.

There is international agreement that, in principle, customary international law also applies in cyberspace. Nonetheless, international dialogue is needed on the question of how international law applies. At present, no UN conventions or global agreements deal specifically with state activity in cyberspace. Important decisions concerning the development and management of the internet are largely being made by commercial and other parties without the direct involvement of governments or citizens. Globally, opinions differ as to the right direction to take on these issues.

The Norwegian Government considers it important for Norway to have a comprehensive, coordinated policy for influencing developments in international cyberspace wherever possible. The Government therefore emphasises close collaboration between official bodies that represent Norway in arenas for the development of international cyberspace framework conditions and rules. In the white paper St. meld. 37 (2014-2015), the Government discussed global security challenges in the area of foreign policy. In response to the white paper, the Ministry of Foreign Affairs established a national cyber-coordination group in 2016, which is tasked with synchronising Norway’s cyber policy positions in international forums.

Our international cyber policy is designed to serve Norway and Norwegian interests, secure robust, predictable framework conditions, and help prevent and protect against challenges and threats in cyberspace. Stronger national coordination will improve the effectiveness of our policy and help boost our international reputation in this field. This international cyber strategy is an important first step towards better national coordination in this area.

Oslo, 31 August 2017

Contents

Introduction

Over a very short space of time, the internet has altered the global landscape of which Norway is a part. It has become the world's most important piece of infrastructure, facilitating global exchange of goods, services and information. In the very near future, the internet is expected to become the superstructure on which all other infrastructure depends. Cyberspace is of great and increasing importance to national economies, security, growth and development.

In response, countries have intensified their efforts to promote national interests in the development and use of cyberspace, through multilateral processes in forums such as the UN, NATO and OSCE, through bilateral usage and regulatory processes, as well as through security policy dialogue between allies and in global forums for the development of international trade, justice and transport policy. Contact and cooperation are also being pursued with the private sector.

Unlike in other areas of great importance to the global economy and global security, no UN conventions or global agreements currently deal specifically with the regulation of national activities in cyberspace. Although there is international agreement that, in principle, customary international law also applies in cyberspace, there is some doubt and disagreement as to how and when international law applies.

Norway's economy and security depend on a well-functioning global internet and robust global digital infrastructure. Norway has a fundamental, long-term interest in contributing to create good and predictable conditions for the future development and use of cyberspace.

Defence against digital threats is becoming ever more important. However, defence alone is no guarantor of security. As in the analogue world, the underlying causes of threats need to be addressed, and remedial measures must be weighed against the many benefits and opportunities offered by cyberspace. It is important to find the right balance between security and openness. The proper functioning of cyberspace requires both.

Background

Cyberspace provides a foundation for national and global innovation, growth and development. With stable, robust digital infrastructure in place, there are almost no limits to what the internet can facilitate. Over the past 20 years, the internet has impacted on most spheres of society. Manufacturing, trade, entertainment, education, finance, health services, agriculture, communications, political activism, transport, media, security and interaction with public agencies are just some examples of this. The internet will continue to play an important role in social and economic development in the years ahead, particularly in developing countries.

Although central government plays a limited role in the *development* of cyberspace, the state has an important function as a *facilitator* of development, for example through innovation, research, teaching and ownership and protection of critical infrastructure. Internationally, national authorities are key players in the development of standards for cyberspace, both politically and operationally. However, the evolution of the internet and digital product and service development are primarily being driven by private companies and research and development institutions. Moreover, the backbone of the internet – global digital infrastructure – is largely in private hands. The Government considers private ownership to be positive in principle, as it promotes competition and continued innovation and development. On the other hand, important decisions relating to the development and security of cyberspace are largely being made by commercial and non-state actors outside traditional inter-governmental arenas.

Society's growing dependence on cyberspace has been accompanied by a sharp increase in digital security challenges and digital vulnerabilities. Cybercrime and network operations originating from both state and non-state parties represent very serious threats to Norway's security and economy. This must be reflected in Norway's international cooperation and security and foreign policy. The present cyber strategy document sets out Norway's governing principles and strategic priorities for this area.

Governing principles

The sustainability of the global internet is dependent on a proper balance between *openness, security, robustness* and *freedom*. International cooperation is key in this regard.

Norway's aim is that cyberspace should promote innovation and international trade, support global stability and security, and safeguard democratic values and universal human rights. This objective is pursued in collaboration with other countries and international organisations, as well as non-governmental partners such as academic institutions, technical research centres, businesses and civil society.

Cyberspace is influencing all spheres of society. The Government is therefore giving priority to close coordination between relevant official bodies that represent Norway in arenas for the formulation and development of international cyberspace policy.

Openness

The success of the internet can be traced to its interoperability, open access and consensus-based international standards. It is vital that both public and private internet administrators keep abreast of developments and the latest innovations. Public regulatory intervention must safeguard continued openness, and not restrict innovation and creativity on the part of developers, entrepreneurs and other stakeholders.

Security

Norway will protect its digital networks, and work with other countries to provide a secure cyberspace that promotes confidence in public authorities, businesses and individuals. Cyberspace security demands a proper balance between what *can* be done and what *should* be done to reduce society's vulnerability.

Robustness

The network of networks that comprises the internet crosses geographical boundaries. Global development is dependent on the stability of and confidence in digital networks. Network security is not solely a technical issue. It is important to clarify the allocation of responsibility between the authorities and the private sector. International agreement is required on respect for technical infrastructure in both peacetime and conflict. End users must be held responsible for the safe handling and operation of their digital devices.

Freedom

Democratic values and individual rights must also be safeguarded while protecting digital security interests.

Universal human rights also apply online. It is important that human rights such as freedom of expression, freedom of assembly and freedom of religion enjoy the same protection in cyberspace as elsewhere.

Norway's strategic priorities

Cybersecurity: promoting secure, stable and robust digital networks

Norwegian society is reliant on secure, stable and robust digital networks to function properly. This also includes basic social functions such as energy supply, water supply, health services, transport, public security and the financial markets. Cybersecurity requires broad cooperation between stakeholders, across national borders. To promote secure, stable and more robust digital networks, the Government will:

- **Promote international cybersecurity collaboration and agreement on governmental conduct in cyberspace.** Today Norway participates in important arenas under the auspices of the EU, UN, OECD (Organisation for Economic Co-operation and Development), OSCE (Organization for Security and Co-operation in Europe) and Council of Europe, as well as bilateral and regional dialogues with other countries, including in the context of Nordic cooperation.

- **Build global understanding of the need for an integrated approach to personal, technological and organisational security measures.** Norway will seek to be an example for other states seeking to facilitate productive interaction between digital access providers, suppliers of goods and services and regulatory authorities in order to identify digital threats and deal with cyberspace incidents. It is the responsibility of the authorities to foster a robust security culture that supports human digital conduct.

- **Intensify international cooperation to build capacity to discover, report and deal with serious incidents in cyberspace.** Digital attacks and incidents span national borders, and their prevention and resolution therefore require international cooperation. The Government will continue to develop its collaboration with other countries to improve its own, and partners', capacity to avert and deal with digital attacks.

- **Promote international standards and cooperation.** Electronic communications are global in nature. Products and services consumed in Norway are very often manufactured and developed in other parts of the world. To contribute to the development of good international standards is therefore in Norway's interest. The European Network and Information Security Agency (ENISA) and the European Telecommunications Standards Institute (ETSI), as well as the latter's Technical Committee Cyber (TC Cyber), are important partners at the European level. Globally, the International Telecommunication Union (ITU) is a key figure in cross-border cooperation.

- **Advocate the adoption of a common European basic security level.** The production of Norwegian electronic communication services is largely dependent on physical infrastructure and inputs from suppliers outside Norway. Norway will promote the adoption of an appropriate European regulatory framework that addresses security challenges linked to outsourcing and internationalisation and includes and control of suppliers and cross-border cooperation.

- **Strengthen cooperation with the EU.** Cooperation with the EU in the field of cybersecurity is of great importance to Norway. The Government will maintain its efforts to optimise this collaboration, including by implementing the Directive on Security of Network and Information Systems (the NIS Directive) and working with the European Network Information Security Agency (ENISA). Norway will also participate in the contractual Public Private Partnership on Cybersecurity (cPPP Cybersecurity).

Innovation and the economy: promoting innovation, development and market access

The digital economy continues to expand rapidly, and is a prime driver of value creation, innovation, competitiveness and growth. Cyberspace is fostering growth and employment by providing a foundation for investment and innovation, securing access to larger markets and reducing the importance of geographical location. Even small businesses can now reach customers all over the world at no significant additional cost. To ensure that cyberspace continues to benefit the Norwegian economy and encourage innovation, the Government will:

- **Promote global openness on the internet.** Norway will work with other countries to ensure that the internet remains an open and non-discriminatory communication platform that fosters consumer confidence in digital markets.

- **Facilitate digital innovation** in the private and public sectors in the EEA. Norway will also give priority to improving digital expertise and digital skills to meet future employment market needs.

- **Protect intellectual property.** In cooperation with other states, Norway will help to protect copyrighted works and sensitive information against theft and reproduction, and encourage actors in the Norwegian information security sector to join the European Cyber Security Organisation (ECSO).

- **Promote Norwegian research globally** to ensure that Norwegian researchers are at the forefront of information and communications security developments. To ensure high-quality Norwegian research in the field of ICT security, the Government will facilitate close collaboration with leading international researchers and knowledge centres.

- **Support growth of the digital economy in cooperation with other OECD member states.** Norway's priorities will include improving access to digital services globally, reducing barriers to investment in and use of digital technologies, promoting commonly agreed global standards for an open, stable and accessible internet, supporting the development of national and international strategies for privacy and data protection, developing and applying technology-neutral regulations that foster infrastructure competition, reducing obstacles to global ecommerce development – with an emphasis on increased consumer confidence – and improving education and training systems to meet demand for ICT expertise. Norway will also participate in coordinated research and innovation efforts in the ICT security field in the context of EU/EEA cooperation.

Crime prevention: international cooperation to combat organised cybercrime and other serious crimes committed through cyberspace

The digitisation of society has created new arenas for criminal activity, including financial crimes, sabotage, sexual assaults and encouragement of violent extremism. Norwegian businesses and interests are under increasing pressure. Digital networks can be both a channel for criminal activity in cyberspace and a target in themselves.

Norway will participate actively in international efforts to combat cybercrime, by:

- **Contributing to the development of standards, conventions and measures to combat cybercrime.** Norway has a long-term strategic interest in influencing the development of international conventions, international standards and other measures constituting the framework for global anti-cybercrime efforts. In this context, it is important to ensure effective international criminal prosecution, and Norway will therefore seek to encourage wider adoption of the principles in the Council of Europe Convention on Cybercrime (the Budapest Convention). Norway's priority is international harmonisation of cybercrime legislation, as well as effective cross-border assistance and crisis management mechanisms.

- **Participating actively in international police cooperation in the field of cybercrime.** Norway is committed to cooperation through Europol, Interpol and Nordic mechanisms to support the exchange of expertise and information and capacity-sharing. Norway will give ongoing consideration to the need for local liaison officers in major international Europol and Interpol projects, and second specialist personnel for defined periods. Virtual ICT services and cross-border dissemination of data and software are providing safe havens for cybercriminals, and Norway will continuously evaluate the need for closer cooperation with other countries to shut down such havens.

- **Strengthening and further developing measures to combat online radicalisation and recruitment.** To prevent radicalisation and violent extremism, Norway will work with other states to develop measures targeting platforms that spread extremist propaganda. Norway will collaborate closely with countries facing similar challenges, and ensure that its own measures meet high international standards.

- **Participating actively in arenas for international exchange of information and experience and development of robust solutions for the prevention and combating of cybercrime.** Participation in such forums facilitates the sharing of experience that is valuable in Norway's policy development and efforts to combat cybercrime. Norway's experiences may likewise be helpful to other countries. Relevant international arenas include the United Nations Office on Drugs and Crime (UNODC), the Council of Europe, the EU, the Internet Corporation for Assigned Names and Numbers (ICANN), ENISA and Eurojust.

Cyberspace as a security policy issue

Norway must be protected against serious digital threats from state and non-state actors. Freedom of action in cyberspace must be secured by means of both national measures and international cooperation, particularly within the framework of NATO, the OSCE and the UN. NATO is an important forum for the exchange of experience and expertise, development of common standards and joint exercises and training to enable allies to operate together during crises. It is also key in the ongoing development of cyberspace as an operational domain. The OSCE is working on "ground rules" and confidence-building measures, while discussions in the UN context are focused on the application of international law and, increasingly, the dilemmas and challenges raised by the development of cyberweapons. Norway will pursue national and international measures to protect its security policy interests, including the following:

- **Continue to develop strong national safeguards against cyber threats, not least through broad civilian-military and public-private cooperation. Norway will invest further in intelligence.** A prerequisite for robust protection against digital attacks in peacetime, crisis and war is the ability to detect, resist and manage threats, including through relevant countermeasures in accordance with international law. A further key factor is capacity to counter digital attacks within the framework of international law. Cyberattacks lose some of their utility value when the opponent is prevented from achieving the desired result.

- **Improve digital-attack defence capabilities in cooperation with likeminded countries.** Priority will be given to NATO and bilateral and multilateral collaboration with close allies. Norway will protect Norwegian forces deployed in international operations against digital attacks, and will work with partner countries when this serves Norwegian interests. Norway will reinforce NATO's collective capability to manage digital threats by developing national capabilities, engaging in multilateral cooperation between allies and supporting NATO processes to improve robustness, exploit technological opportunities and enhance crisis management capacity. Norway will also help raise awareness of the dilemmas and challenges identified in the development of military cyberspace capabilities, including questions such as arms control, export control, delimitation of state and non-state actors, and attribution.

- **Explore the application of international law in cyberspace.** Although there is an international consensus that international law also applies in cyberspace, there is a need for clearer international agreement as to how and when international law applies. The work of the United Nations Governmental Group of Experts (UNGGE) and the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn are important in this regard.

Global internet governance: promoting efficient, stable and inclusive structures

The internet is a complex piece of global infrastructure. No single entity controls the internet. Moreover, there are no internationally binding agreements that regulate how countries should respond to specific challenges arising in the context of internet development. However, both the global organisations that control key internet resources and relevant authorities are showing increasing interest in the development and adoption of principles for good resource management and administration. Both private bodies and authorities are involved in these vital efforts to prevent the internet from becoming fragmented and losing its global nature.

Robust resource management and principles for internet administration and development – internet governance – are thus growing in importance. Confidence that services delivered via the internet are stable and secure is a fundamental prerequisite for continued internet and service expansion. In order to promote robust global governance of the internet that fosters effective, stable and inclusive structures, the Government will:

- **Help ensure that the internet remains an open, accessible and robust platform for growth and social and cultural development.** Norway will work with other countries to promote a global internet policy that encourages innovation and the development of content, applications and services. Norway will engage actively in international arenas serving this aim.

- **Promote the principle of role clarification.** In collaboration with other countries and the business sector, Norway will promote the principle that businesses should generally bear operational responsibility for internet operation and maintenance, while administration should fall to the so-called “multi-stakeholder community”, which includes not only the authorities but also businesses, civil society and academic institutions.

- **Promote robust management.** Norway will in cooperation with other states seek to refine the multi-stakeholder model and emphasise and promote good management principles such as openness, responsibility, transparency, representativeness and impartiality among the organisations that control fundamental internet resources.

- **Avoid unnecessary governmental intervention.** Norway will work with other countries to avoid official regulation of the internet that hinders development, innovation and communication, or that facilitates censure and the dissemination of propaganda.

- **Promote openness and freedom.** In collaboration with other states, Norway will seek to ensure that the internet remains an open and freely accessible arena in which all individuals can disseminate and receive information, and in which fundamental human rights are protected. Breaches of universal rights can never be justified by national or global internet governance objectives.

Development: internet access and capacity development to utilise the potential offered by cyberspace to promote growth, prosperity and security for all

Norway has an important global role to play in supporting capacity-building in the cyber field in other countries and regions, in line with several of the UN's sustainable development goals as defined in Agenda 2030. Developing countries must be given greater opportunity to benefit from the possibilities presented by the internet, and be enabled to deal with digital challenges and threats.

To achieve these objectives, the Government will:

- **Promote and support capacity-building in the cybersecurity field in developing countries.** In this context, capacity-building includes institution-building (e.g. national telecommunications authorities and national computer emergency response teams (CERTs)), e-government, cybercrime investigative capacity, development of national electronic communications laws, innovative solutions for health and educational assistance, development of digital infrastructure and the establishment of warning systems. As part of these efforts, Norway will intensify its collaboration and dialogue with the EU on cybersecurity capacity-building in non-EEA countries.
- **Give greater emphasis to robust infrastructure and security and openness in cyberspace as part of the sustainable development agenda,** in the context of the Government's global efforts to combat poverty and promote trade, social and economic development, education, health care, human rights and democracy. Norway will also support achievement of the UN's sustainable development goals relating to infrastructure and innovation.
- **In cooperation with international institutions, seek to enable more developing countries to exploit the opportunities offered by the internet for economic and social development,** including job creation and access to educational and health services. This includes helping developing countries to improve internet access and building expertise and capacity to prevent, detect and deal with digital threats, cybercrime and illicit financial flows using online tools. In doing so, Norway will also contribute to achievement of the UN sustainable development goals relating to peaceful and inclusive societies. Norway will work with others to close the gap between women and men's access to and use of the internet, to give women equal opportunity to participate economically and politically in social development.

Online freedom: universal rights also apply in cyberspace

Norway will help ensure respect for international human rights in global cyberspace, by:

- **Supporting proponents of freedom of expression in cyberspace.** In cooperation with likeminded countries and civil society, Norway will help to maintain and develop platforms that facilitate free expression and association in cyberspace.

- **Promoting greater understanding of the importance of cybersecurity.** Secure communication solutions and cybersecurity are important for human rights activists, journalists and others who may be monitored due to their opinions and statements.

- **Working with other countries, the business sector and other non-governmental actors to ensure that as many people as possible have access to a free and secure internet.** One means of doing so is continued engagement in the *Freedom Online Coalition.*

- **Building global understanding of the importance of protecting the right to privacy in cyberspace.** This includes promoting the principle of lawful, proper and proportionate surveillance.

Published by:
Norwegian Ministry of Foreign Affairs

Public institutions may order additional copies from:
Norwegian Government Security and Service Organisation
E-mail: publikasjonsbestilling@dss.dep.no
Internet: www.publikasjoner.dep.no
Telephone: + 47 222 40 000
Publication number: E-969 E
Print: Trykkerinavn 03/2018 – Impression 200

MILJØMERKET
2041 0446
Trykksak