Sweden in a digital world

A strategy for Sweden's foreign and security policy on cyber and digital issues

Table of contents

Foreword

Cyber and digital issues are growing in scope and importance as an item on the foreign and security policy agenda. The emergence of new strategic digital technologies such as artificial intelligence, quantum technology, advanced semiconductors and next-generation communications networks (6G) is a key factor in international cooperation and the global balance of power. By virtue of its role as a leading global actor, and with a wide range of instruments available to it, the EU is Sweden's most important foreign policy platform also in relation to cyber and digital issues.

Sweden will pursue a policy based on solidarity within the scope of the European Union (EU) and the North Atlantic Treaty Organization (NATO). Based on our interests and values, Sweden will be a key actor in international contexts, including in relation to strategic partners. Cooperation with the private sector on international and cross-border threats and attacks is also an important part. To strengthen its role and influence internationally, it is crucial that Sweden pursues a coherent and integrated foreign and security policy on cyber and digital issues. All aspects of foreign policy are concerned– security, trade and development assistance. It is in that light that this strategy should be viewed. Ultimately, it is a matter of safeguarding Sweden's security, prosperity and competitiveness.

For the Swedish Foreign Service, efforts on cyber and digital issues are about promoting Swedish innovation and industry, promoting Swedish values and interests, strengthening development cooperation, and deepening security policy cooperation with the aim of strengthening Sweden's capacity to respond, resist and deter, with a focus on malicious state actors.

This strategy aligns with the Government's national security strategy. It is also designed to be mutually reinforcing with the national cyber security strategy which will be adopted in 2025. National capabilities and foreign and security policy instruments are closely intertwined. Through a comprehensive approach, Sweden stands stronger.

Maria Malmer Stenergard

Minister for Foreign Affairs

A digital world

The international system is rapidly changing, with cyber and digitalisation issues now constituting a key part of global development. It is less and less meaningful to differentiate between digital and physical reality, and this also applies to the area of foreign and security policy. The geopolitical dynamics playing out in the physical world are mirrored in the digital environment.

Increasingly, network and information systems are forming the underlying infrastructure of all parts of our societies. The expansion of 5G/6G is making this dependence on digital infrastructure and the development of future generations of telecommunications infrastructure even more profound.

This development demonstrates that technology, economics, democracy and security are increasingly intertwined in international relations. Emerging technologies, such as artificial intelligence, are expected to have a decisive impact on power dynamics and geopolitical competition. Security policy must address threats in new domains, where critical services can be disrupted remotely without kinetic action, and the cost of engaging in malicious influence operations is negligible.

The digital economy is becoming increasingly important to national prosperity and a more pronounced part of geopolitics. Digitalisation can help lift countries out of poverty and contribute to technological leaps. However, digital development that is not based on democratic values can instead foster increasingly authoritarian societies.

Public and private actors in Sweden are regularly subjected to cyber attacks from foreign powers. Our capacity to manage and respond to malicious cyber threats to key systems and services is therefore vital. Effective deterrence in the cyber area is achieved through credible resilience and the capacity to take measures in response.

This strategy lays the foundation for a coherent and integrated foreign and security policy on cyber and digital issues, and ultimately aims to safeguard Sweden's security, prosperity and competitiveness. Sweden's overarching priorities are about consolidating a global, open, free and secure cyberspace based on the rule of law. The EU, NATO, bilateral strategic partnerships and cooperation with the private sector are particularly important if Swedish interests and priorities are to gain traction.

1.Security policy

Sweden faces a number of challenges in the area of cyber and digital issues that need to be addressed, integrated into and managed in a security policy context. This means promoting Swedish innovation and industry, promoting Swedish values and interests and deepening

security policy cooperation on new technologies. The aim is also to strengthen Sweden's resilience and its capacity to deter and respond to external cyber threats, with a focus on malicious state actors.

Strategic digital technologies

The emergence of new strategic digital technologies such as artificial intelligence, quantum technology, advanced semiconductors and next-generation communication networks (6G) will be a key driver in global politics and influence international cooperation and global power dynamics. Control over technology and data, as well as the requisite raw materials, components and know-how, is used more frequently as an instrument in geopolitics. This has consequences for production, world trade and global value chains.

In particular, the developments in AI needs to be understood from a geopolitical perspective. From a security policy point of view, the extensive investments now being made in AI research and relevant applications will affect the future balance of power between states. A kind of AI race has begun, not unlike that in other areas of technology with security and defence policy applications. While the use of AI has great potential to contribute to solutions to global challenges, there are also risks that require both regulation and international cooperation.

Sweden is a prominent country in research and development of new technologies and is well placed to be in the forefront in many areas, and influence the development of regulations, norms and standards for new technologies. International cooperation and partnerships are central in research and innovation, and necessary to ensure access to skills, technologies, capital, raw materials and components. Sweden must be regarded as a competent and dependable partner in the management, use and control of critical technology, and in the development of global standards, norms and regulatory frameworks.

There is significant foreign interest in Swedish technology development. This interest is positive and leads to commercial joint ventures and foreign direct investment. But there are also challenges in terms of acquisition of Swedish companies (in particular research-intensive small companies) and, to a greater extent than previously, industrial espionage. It is therefore necessary to protect national security interests.

At the same time, the rapid development of dual-use technologies gives rise to new challenges from an export control perspective in managing emerging critical technologies. In many cases, such technologies are not yet listed in the international export control regimes (e.g. the Wassenaar Arrangement) which requires states, including Sweden, to protect their technology at the national level to prevent its proliferation to undesirable recipients.

The ongoing development of the internet is closely tied to the emergence of new digital technologies and itself constitutes a strategic interest. Sweden will continue to work for an open, global and interoperable internet that is governed through multi-stakeholder

cooperation. Authoritarian countries' ambition for increased state control, including at a global level, must be countered.

Foreign and security policy management of cyber threats and cyber attacks

A number of countries carry out cyber attacks on Sweden. The capacity to manage cyber threats and cyber attacks is fundamental to Sweden's security. Cyber attacks can entail intelligence gathering of various kinds, but also activities that aim to affect or manipulate access to various services and systems or even to destroy them. These attacks are carried out as one of several different instruments in hybrid operations to manipulate Sweden and harm Swedish interests. In addition, Sweden must assume that more powerful offensive cyber attacks may be directed at targets in Sweden in the event of further deterioration in the international security situation.

Sweden will pursue a policy based on solidarity within the EU and NATO. The rules-based world order and respect for the Charter of the United Nations and international law are continually fundamental to our foreign policy. In view of the heightened geopolitical tensions and the cross-border nature of cyber threats, as well as the continued rapid digitalisation of Swedish society, the cyber and digitalisation area must be fully integrated into Sweden's foreign and security policy. These issues are dealt with bilaterally, within the EU, NATO and the Organization for Security and Co-operation in Europe (OSCE), as well as in the broader context of the UN.

Sweden's foreign missions play an important role in contributing to Sweden's overall situational awareness. Sweden will remain a driving force in the development of foreign policy and diplomatic toolboxes to respond to threats and attacks – against Sweden, the EU and NATO. Sweden will also continue to participate actively in the development of international regulatory frameworks, recommendations and policies with the aim of enhancing our common cyber security and strengthening resilience in the cyber area. Effective law enforcement at EU level and internationally is also essential. It is important to strengthen skills in the Swedish Foreign Service, and to further develop cooperation between the Swedish Foreign Service, the responsible ministries and the relevant government agencies concerning cyber and digital issues.

Work to directly and indirectly address malicious state actors includes:

i) Countering cyber threats and cyber attacks

International cooperation is fundamentally important to counteracting threats to peace and our security, including in the cyber area. For Sweden, the main avenues for this cooperation should be within the framework of the EU and NATO in collaboration with other like-minded states. It includes cooperation and information-sharing concerning situational awareness, principles and procedures for public naming and attribution, and various types of foreign policy responses such as public statements and targeted sanctions.

Cooperation within the EU and NATO and with strategic partners contributes to deterrence and resilience. Like NATO, Sweden has concluded that, under certain conditions, cyber attacks can be equated with an armed military attack.

ii) Strengthening resilience and improving capacity in the cyber area through international cooperation

International cyber security cooperation within the framework of the EU and NATO, for example, is also an important part of the efforts to strengthen resilience and improve capacity in the cyber area internationally and nationally. International regulatory frameworks, as well as recommendations and policies, support measures to create a high level of common cyber security. In international cooperation, Sweden will advocate for measures that strengthen and streamline cooperation in the area of cyber security, with the aim of enhancing our common cyber security.

iii) Strengthening the application of international law and human rights law in the cyber area

Sweden strives for global compliance with a rules-based world order. International law, including the entirety of the Charter of the United Nations, international humanitarian law and human rights also apply to the cyber area. However, there is a need to closer analyse how the rules of international law should be interpreted and applied in a cyber context. Sweden will act to ensure that international law is respected and applied in cyberspace. Sweden will be a driving force in international discussions on the application of international law in the cyber area.

iv) Acting to support norms of responsible state behaviour

Besides binding rules of international law, a number of non-binding norms and principles have been developed. This discussion has progressed furthest within the UN, where eleven non-binding norms and principles of responsible state behaviour in cyberspace have been agreed upon. These concern fundamental issues such as the protection of critical infrastructure, individual privacy, countering terrorism and criminal or harmful information and communication technology (ICT) activities, and international cooperation. These norms now constitute an important starting point for how states should behave in relation to each other in cyberspace. This framework also provides the foundations for better dialogue and supports accountability. Sweden will work to ensure that existing norms are respected and applied, and in relevant cases further developed for example based on, the global development and new technologies.

v) Strengthening measures to build confidence and trust

The risk of misunderstandings about the underlying causes of incidents or failures in network and information systems is high. System errors, operator errors and incidents in interoperating systems very often have the same kinds of outcomes as those of a cyber attack. The technical analysis then required is often complex and time-consuming. The lack of

international transparency and understanding of different uses of terms and concepts around cyber security increases the risk of conflicts. Both the UN and the OSCE have therefore adopted a number of measures to build confidence and trust in the cyber area. Sweden is working to ensure that these will be solidified, implemented and developed. Cooperation between incident management and law enforcement activities in the investigation of disruptions and incidents within the framework of international security partnerships or cross-border cooperation between government agencies often leads to increased transparency. This contributes to increased trust and confidence between parties and the ability to identify the actual causes of disruptions more rapidly. Sweden wants to contribute to intensifying international partnerships on practical measures to build confidence and trust.

vi) Safeguarding the flow of digital information

The free flow of information on the internet is used more frequently for malicious purposes. One central issue is how democracy and its institutions and processes should be defended against information influence by malign actors while countering repressive demands for restrictions on free information flows. State actors, such as China and Russia, as well as violent extremist groups, networks and individuals, use the internet and social media to spread propaganda and disinformation. AI that is used to filter and generate content risks reinforcing polarisation and having a negative impact on conflict situations within and between states. The EU has taken important steps to become a global normative actor in this area. But there are also actors who want to use the growing debate about the influence and power of these platforms to push through more repressive norms. Sweden will act to ensure that emerging norms and rules are based on international law, include a rights perspective and are based on democratic principles, and contributes to favourable conditions for innovation and increased competitiveness. Sweden will prioritise the increased protection of democratic institutions and processes from malign and harmful information influence to a greater extent. It is particularly important to pay attention to the impact on electoral processes, with a view to the entire electoral cycle – nationally as well as at global level.

vii) Promoting international cooperation to combat system threatening cyber crime

International cyber security discussions in foreign policy focus mainly on threats from state actors. A large proportion of cyber crime is cross-border and often involves multiple actors. There are many examples of organised crime actors with close, but concealed, ties to malicious state actors. By deliberately failing to intervene against organised cyber crime conducted from their own territories, states may also use such groups as a security policy instrument. There are also examples of state actors using methods and tools from the cyber crime area to conceal their activities. The boundary between non-state and state actors is thus often blurred.

Cyber crime is a cross-border problem, often with security policy dimensions, that requires increased international cooperation to prevent and combat effectively. Effective law enforcement, within the framework of rule of law, is a prerequisite for upholding

fundamental rights and ensuring that the cyber area is not a refuge for criminals. Sweden will continue to take an active role in international cooperation to counter cyber crime, particularly on the basis of joint action within the EU and including in foreign policy cooperation. But it is also important that new instruments respect the rules of international law, including human rights, and are not used to increase states' control over central internet infrastructure, or to legitimise and facilitate repression.

Focus areas – Security policy

- Develop Sweden's international cooperation around AI and other strategic new technologies, including security aspects, with prioritised partner countries, organisations and actors.
- Promote cooperation and interoperability regarding rules and standards between the United States and EU and in multilateral forums. Defend the internet governance model based on multi-stakeholder participation.
- Within the framework of the EU and NATO, develop Sweden's capacity to deter and respond to external cyber threats and cyber attacks using foreign and security policy instruments. This includes further national coordination on situational awareness, attribution and response measures.
- Support the implementation and ongoing development of measures to build confidence and trust, multilaterally within the UN and the OSCE, and through partnerships with other countries.
- Work to ensure that international law and existing norms are respected and applied in cyberspace.
- Develop dialogue and cooperation with the private sector on global norms for new technologies and international cooperation on cross-border threats and attacks.
- Support international cooperation on export control and investment screening within strategic technologies.
- Develop skills within the Swedish Foreign Service on cyber and digital issues.

2. Trade, prosperity and competitiveness

Sweden is one of the world's leading nations within digital development. The digital economy is central to Sweden's economic development, including Sweden's competitiveness and position in the internal market and globally. Promoting Swedish digital technologies and improving the conditions for businesses to operate in an international market is a central task for trade policy. But recent geopolitical developments also emphasise the importance, when it comes to cyber and digital issues, of pursuing a consistent and integrated policy with regard to trade and security.

Trade and security as integral parts of Swedish foreign policy

Innovation linked to digitalisation and new technology has long been a central economic and trade policy interest for Sweden. Swedish companies are at the forefront of the innovative development and use of digital technology that can contribute to solutions to major global challenges. However, Sweden operates in a global market where many countries make significant investments in research and development of new and advanced technologies. There is a global demand for technology developed by Swedish businesses, and within certain strategic sectors Swedish businesses have considerable standing. This gives Sweden an influence, but also underlines the importance of safeguarding and promoting this capacity for Sweden's future economic base. Digital products and digital trade have an increasing impact on the basic functioning of society. An integrated approach to these issues increasingly entails foreign and security policy considerations.

Goods and services with digital content are manufactured, sold and used in a global market today. Sweden will work to protect the global market from products and software with substandard security functionality or that could pose a security risk – particularly in relation to authoritarian states. Essential services rely on digital technology, which imposes new demands on improving cyber security. Laws, rules and standards are important for strengthening cyber security in general, but can also result in increasingly national or regional preferences and restrict openness in the form of trade barriers to digital development. Sweden wants to minimise regulation's negative effects on trade and safeguard its compatibility with the WTO rules.

In cyber and digital matters, Sweden's trade and security policy interests should be addressed in a comprehensive manner and, as far as possible, be mutually reinforcing.

Public-private partnerships

The private sector accounts for the majority of the funds spent on digital research in Sweden and is a driver in technology development. Competition between countries to attract business investment and high-level skills is increasing, especially in research and innovation concerning advanced technology. Private companies have an increasing influence on security, the mechanisms of democracy, the labour market, innovation, and the media landscape. Sweden has a powerful and innovative digital technology sector of global eminence. Today, it not only forms an important part of Sweden's economic base but can also make significant contributions to finding solutions to global challenges. Cooperation and the sharing of best practices concerning innovation and technology can strengthen bilateral partnerships, streamline development collaborations in the digital sector, create export opportunities and contribute to making Sweden an attractive investment nation.

Private sector participation in international cooperation forums, for example within the EU, NATO and the UN, contributes positively to initiatives for international standards and rules, and more cooperation like this should be encouraged.

Development of the EU and the digital internal market

The EU is a leading global actor on regulation and norms in relation to cyber and digital issues. Sweden is working to make European approaches globally normative. Within the EU, the question of open strategic autonomy, and its digital counterpart digital sovereignty, have been the topic of frequent discussions. The overall goal of the Digital Decade is to make the internal market fully data-driven by 2030, with the EU establishing a model for data use centred on the interests of the individual and European values. Sweden is working to make the EU a stronger actor in the digital area. The discussion on economic security and resilience will continue and Sweden must be part of these discussions with the goal of increased resilience and continued openness – as well as decreased vulnerabilities and perilous dependencies, especially in relation to authoritarian states. However, the aim must be to focus on cooperation and transparency in relation to third countries as well. Any restrictions must be carefully considered so that they do not weaken Swedish interests and national competence. Sweden takes the view that increased European research and innovation capacity will benefit from open global cooperation. Sweden should act to achieve digital sovereignty in an open market and in cooperation with strategic partners, with a view to counteracting regionalisation and fragmentation that might otherwise have economic and security policy consequences.

In June 2023, the European Commission published its Joint Communication on a European Economic Security Strategy. The Strategy highlights the tensions between strengthening economic security and ensuring that the EU continues to benefit from an open economy.. In working with these processes, Sweden welcomes a balanced approach in which the EU strengthens security while we reinforce Europe's long-term competitiveness and productivity. Any negative effects of strengthened security on the internal market and global institutions, including negative effects on the openness and free trade on which Sweden's prosperity depends, must be limited as far as possible.

The internal market strengthens the competitiveness of Swedish businesses. Europe should fully utilise the benefits from the innovation and creative power that societies with freedom and competition brings with it. The D9+ group, of which Sweden is a part, is an important network for cooperation and represents an opportunity to influence and lead the digital agenda at EU level. The European Commission has presented a series of proposals aimed at regulating structures and actors in the digital landscape. The value of data is to be fully realised in line with the European data strategy. Substantial investments in the technical structures that are to underpin the regulations are made through strategic projects in funds and programmes such as Horizon Europe, the Connecting Europe Facility and the Digital Europe Programme. These EU rules for digital services and goods affect both the internal

market and external trade with non-EU countries. Sweden welcomes in principle regulation that would strengthen predictability. Sweden wants the legislation to be preceded by impact assessments so that it does not hamper businesses' competitiveness and innovation. The aim should be regulatory frameworks that are interoperable with strategic partners' systems.

Security of supply in strategic technology areas

Digitalisation has made the global economy increasingly dependent on certain strategic products, minerals and technologies. This is particularly true for Sweden, which is a trade-based, innovation-based and digitalised economy focused on a global, green, secure and digital transition. This places new demands on Sweden to act strategically when interests motivated by trade policy on the one hand and security policy on the other come into conflict.

Globally, particular attention is being paid to the communication technology of the future. Digital telecommunications are a kind of circulatory system, required for societies, economies and states to function, and thus are of great strategic importance. The fact that one of a few trusted suppliers has their research activities concentrated in Sweden is of significance for more than just export promotion. It gives Sweden a role and a responsibility to act strategically and coherently in foreign and security policy dialogues and processes, as well as in those concerning trade policy. Particular attention now needs to be paid to next-generation systems (6G etc.) and to the conditions for security, research and innovation, as well as to central government interventions that affect competition and the level playing field. Fundamental principles of the Swedish approach are technology neutrality, stability, security and diversification in ICT value chains, and the importance of global standards.

Infrastructure

Sweden is dependent on international fibre-optic cables for communication with the outside world and, in practice, also for safeguarding national needs for electronic communication and access to digital services. Businesses' competitiveness is dependent on well-functioning connectivity. Physical or cyber attacks on international connectivity pose a significant threat and the changing security situation has brought the vulnerability in both the EU's and Sweden's connectivity with Asia to the fore. It is important for Sweden to promote redundancy and resilience of its digital infrastructure.

Data flows, digital trade barriers and storage

The capacity to manage and realise the value of data is fundamental to the development of new technologies and for trade in both goods and services. This makes functioning and free data flows central to Sweden's and Europe's competitiveness. EU businesses, regardless of size or industry, are increasingly dependent on data flows, and the capacity to capitalise on the value of data is paving the way for completely new businesses and business models.

Conditions for technology development, innovation and trade as well as data protection must be taken into consideration. The conditions for Swedish innovation and technology exports to thrive are improved by providing dimensioned and adapted data protection, including for personal data and immaterial assets.

For data to be used, free flows are not sufficient. From the trade perspective, it is important to combat digital barriers to trade in third countries such as unjustified requirements concerning data localisation and the disclosure of source codes. It must also be possible for data to be processed in a controlled manner, with respect for the rights of individuals, and to be shared and stored stably and securely. This is central to the economic model underpinning most internet and technology companies. The technology industry today makes up an increasing share of the economies of many countries, including Sweden. Without free flows of data and stable and secure data processing, Swedish trade and competitiveness and innovation are at risk. In the longer term, this threatens Sweden's economic security and development. As an innovative and information- and data-intensive country, Sweden needs to be able to pursue these issues internationally in order to safeguard Swedish trade interests. In trade policy, Sweden strives for ambitious regulation of digital trade in EU trade agreements and in plurilateral negotiations on eCommerce in the WTO.

Standards

International standards in the technology and cyber area are central to ensuring that different products are interoperable and can be sold on a global market, which is positive for diversification, connectivity and competition. Sweden has long had a significant influence on international standardisation, since Swedish stakeholders, i.e. companies, government agencies, research and academia, have been well represented in international standards bodies. In recent years, the development of international standards in the technology and cyber area has been marked by increased competition between the great powers. Authoritarian states' increased engagement in standardisation processes has been noted, for example, in questions concerning the internet's architecture and facial recognition technology in the International Telecommunication Union (ITU), but also in the increased presence of state-controlled companies within the International Organization for Standardization (ISO). If the current trend of increased competition continues, it would weaken the multilateral trade policy and market economic principles that have been the basis for the great increases in prosperity of recent decades.

As far as Sweden is concerned, it is crucial to maintain compliance with the WTO Agreement on Technical Barriers to Trade and ensure that standards can maximise the benefits and potential of technology and are non-discriminatory, transparent and technology-neutral. For Sweden, it is important that the regulation of stakeholders and current forms of cooperation for standardisation are safeguarded. At the same time, Sweden needs to actively work against standards being set on the basis of political and strategic motives that are not in line with Sweden's interests.

Cyber security certification

The implementation of the EU Cybersecurity Act means that the EU is developing its own certification schemes within the framework of the EU acquis, thereby facilitating an internal market for goods and services that has an appropriate level of cyber security. For Sweden, it is important to work to ensure that the EU's framework for cyber security certification does not to lead to companies being required to apply for dual and more expensive certifications, with the consequent risk of trade barriers, and of reciprocity applying for market access under different certification schemes. Transatlantic cooperation in the area of cyber security certification is also an important aspect.

Focus areas – trade, prosperity and competitiveness

- Contribute to the work for a stronger, more coherent Europe in the digital area, including a deepening of the EU's digital internal market, open digital sovereignty and strengthened EU cooperation on digital diplomacy (the EU's external digital policy).
- Promote economic security with the aim of strengthened resilience and continued openness – as well as decreased vulnerabilities and perilous dependencies, especially in relation to authoritarian states.
- Through the EU and other international cooperation forums, promote stable and diversified supply chains for strategic technologies, components and input goods.
- Advocate for international data flows to be and remain free-flowing.
- Promote Sweden's digital technology sector and engage in dialogue with the Swedish business sector to harness its expertise and look after its interests in international contexts. Promote exports from Sweden and investments in Sweden in the digital sector. Engage in dialogue with the business sector in order to harness its competence and skills and look after its interests in international contexts in accordance with Sweden's Trade and Investment Strategy.
- Promote the development of dialogue on international norms and rules between governments and the private sector at EU and international level.
- Advocate for the development of international trade-related regulation to conform to the WTO's rules.
- Advocate for ambitious rules on digital trade and data flows in trade agreements, including the plurilateral negotiations on e-commerce in the WTO, together with like-minded EU Member States.
- Contribute to new standards and certifications that simplify and enable increased trade, and to the avoidance of any that may constitute undue barriers to trade or competitive disadvantages for Swedish businesses. Actively pursue regulatory interoperability between the EU and its strategic partners.
- Promote Sweden's capacity to manage a more competitive international standardisation process and to actively defend Swedish positions and interests, including by ensuring that international standardisation bodies remain stakeholder-driven and that the negative

consequences of international competition within the standardisation bodies are minimised.
- Actively participate in the ITU's Standardization Sector.
- Promote Sweden's position as a priority partner for a green and secure digital transformation globally. Sustainable trade in critical raw materials, minerals and other input goods of strategic importance for a green and digital transition must be assured.

3. Development and democracy

Sweden needs to be active in many areas to ensure an open, free and secure cyberspace based on the rule of law.

Digitalisation and democracy

The digital medium creates opportunities to deepen democracy but also makes democracy more vulnerable to various types of digital attacks. Both state and non-state actors are using digital tools and new technologies such as AI as a means to monitor, exercise control over and harass opponents, journalists and human rights defenders, especially women. Protection against digital harassment for these groups must be assured.

Malign information influence undermines democratic institutions, destabilises democracy and increases the risk of political violence. Malign information influence constitutes a threat to an open and democratic society and to the free formation of opinion and must be addressed at both national and international level to protect the core of democracy.

At the same time, digitalisation is increasing the opportunities for civil society and human rights defenders to act, organise and influence. Access to a free, open and secure internet is crucial to promoting political and social participation.

Digitalisation and development

Digitalisation can raise societies out of poverty by providing new opportunities to participate in international trade and global economic development. A substantial part of the infrastructure that enables prosperity is digital. Increased digitalisation thus creates great opportunities for low-income countries to develop. However, large segments of the world's population do not have what is needed to fully benefit from digitalisation and the advantages of digital development. This is especially true for women and girls. Access to the internet is markedly better in democratic countries than in autocracies. An ambitious and inclusive digitalisation agenda can help accelerate the implementation of the 2030 Agenda and the Sustainable Development Goals (SDGs), for example by enabling innovation in areas such as financial inclusion, access to health care, improved agriculture and a better environment and climate. This requires a continued focus on increased and reliable access to ICT.

Development cooperation linked to digital trade (eCommerce) is of great importance to support the participation of developing countries in global trade. eCommerce can create great benefits for small and medium-sized enterprises (SMEs), women, and marginalised groups by reducing export barriers and making more products available at a lower cost. Digital solutions help to break down mobility barriers, discrimination and female entrepreneurs' exposure to violence. But digital development must be accompanied in parallel by systematic work with information and cyber security in order to create resilient societies.

Capacity building and capacity development in digitalisation and cyber security

Support in digitalisation must be accompanied by a strengthening of cyber security capacity. For example, many developing countries lack a national authority whose task it is to support the society in building resilience in the cyber area. At the same time, an increasing proportion of social services, even in areas such as health and education, are becoming digital. An enhanced capacity to build institutions and regulations based on the rule of law, and to build resilience and choose technology using a rights-based approach, is of great importance for broader development in human rights, democracy and the rule of law.

There is a need to expand investment in capacity building in digitalisation, which includes building democratic societies, public institutions and systems for digital administration, and cyber security. Capacity building efforts in both digitalisation and cyber security are therefore necessary. It is in Sweden's interest that countries with which Sweden wants to deepen its political and economic relationships strengthen their resilience to external cyber threats and improve their capacity to strengthen their own sovereignty in cyberspace. In this context, Ukraine is a priority for capacity building in cyber security. Sweden's ambition in the area of capacity development should primarily be coordinated through multilateral initiatives within the EU, NATO, the UN and the OSCE.

Sweden's development cooperation within digitalisation and cyber security

Sweden is working actively to integrate digital components into bilateral development cooperation. This is being done as part of the support provided to promote human rights, democracy and the rule of law, among other things. Swedish development cooperation will support initiatives that promote an open, free and secure internet, as well as initiatives that reduce the digital divide – especially for women, girls and other groups who are particularly vulnerable.

Through its development cooperation, Sweden also intends to contribute to the work to combat malign information influence and to strengthen resilience and increase capacity in digitalisation and cyber security. This includes activities that strengthen and secure the digital tools of organisations and human rights defenders, but also involves raising awareness of the risks and vulnerabilities that increased digitalisation entails. This work also involves raising and highlighting the challenges of digitalisation in everything from threats and violence, illegal trade, malign information influence and cyberstalking to threats to the individual's privacy.

Norms and principles of human rights, democracy and the principles of the rule of law need to guide the development of an inclusive digital administration. Support in the digital area always needs to be accompanied by a cyber security perspective, so as not to create new vulnerabilities.

Sweden's development cooperation supports organisations in their advocacy work to ensure that the internet remains open and secure for individuals, journalists, independent researchers and human rights defenders. This support also includes capacity building, mentoring and training, as well as support in emergency situations such as threats to individuals, internet shutdowns or blocking of communication channels. Support to human rights defenders, including in digital environments, will be developed. In addition, more organisations will receive support in their work to help organisations and marginalised groups in repressive environments by providing them with tools and technology to maintain control over their own information and defend themselves against digital attacks such as malign information influence, agitation, cyberstalking, harassment and violence.

Increased digitalisation facilitates economic development and prosperity and creates major opportunities for development. It is therefore important to promote the opportunities that digitalisation brings for individuals, business and civil society.

The private sector is also an important asset and source of skills in terms of capacity building in cyber security. Enhanced cooperation between the private and public sectors is necessary to be able to develop cyber security as part of development cooperation.

Sweden is therefore reviewing its options for new instruments and financing solutions within the framework of its development cooperation, with the aim of broadening what Sweden offers and increasing the Swedish business sector's participation in digital transformation projects in low- and middle-income countries.

Multilateral cooperation

Sweden's multilateral development cooperation contributes to partner countries' opportunities to take advantage of the potential of digital technology while also being able to manage its risks through strengthened cyber security. Support for policy development, physical investments and capacity development are increasingly being provided through multilateral organisations within the context of the EU, the UN and the development banks. The World Bank Group has an important role to play in reducing the global digital divide. Sweden also contributes support to developing countries so that they can benefit from and meet the challenges of the rapid development of the digital economy.

Digitalisation and gender equality

The unequal distribution of technical skills and access to the internet have particularly negative consequences for women and girls. Sweden is well placed to help strengthen

opportunities and rights for women and girls in the digital area through developing its own capacity-development projects with grants from Swedish government agencies that have cutting-edge expertise in the area. Such initiatives need to target meaningful participation by women and girls throughout the entire chain from the development of technology to its use, including relevant policy decision processes in the technology area.

An increasing number of women and girls are being affected by gender-based and sexual violence, threats, hate speech and abuses on the internet and social media. Digital technologies can also amplify problems of gender-based violence and sexual exploitation of children offline by making it easier to stalk and exploit victims. Violence, threats, hate speech and abuses online have serious consequences; not only for the physical and mental health of women and girls, but also for their opportunities to participate in the democratic conversation.

Focus areas – Development and democracy

- Promote human rights, democracy and the rule of law in digital environments within Swedish development cooperation, for example by ensuring protection and capacity building for human rights defenders, equality, civil society actors, and democracy movements.
- Act to ensure that digitalisation and cyber security become a cross-cutting issue in achieving Sweden's development policy objectives. Sweden's bilateral and multilateral development work should therefore integrate capacity development for digitalisation and cyber security into its framework. This includes helping to ensure digital social services and skills development efforts, and reducing the digital divide between men and women.
- Facilitate synergies between export promotion, trade policy and foreign and security policy in international development cooperation that concerns digitalisation and cyber security.
- Promoting, in multilateral contexts, human rights in the cyber area, especially the rights of freedom of expression, access to information, and privacy.
  Continue to deepen cooperation with like-minded states on digitalisation and democracy, in multilateral as well as bilateral contexts.
- Actively contribute to the ITU's efforts to strengthen the capacity development of developing countries in the cyber and digitalisation area, and promote an inclusive digitalisation agenda to help achieve the SDGs.

4. International cooperation

The EU's cyber and digital diplomacy

By virtue of its role as a leading global player, and with a wide range of instruments available to it, the EU is Sweden's most important platform for its broad foreign policy in relation to cyber and digital issues. In the tough geopolitical competition that surrounds technology and digital issues, a strong, cohesive and open EU is central to promoting Swedish interests, both inside and outside the EU. Overall, the EU's external relations in this area are managed in two tracks: cyber diplomacy and digital diplomacy. Since these are fundamentally different aspects of the same technological development, Sweden is acting to ensure that there is close coordination in the handling of external cyber and digital issues.

Joint EU action is one of Sweden's most effective foreign and security policy tools in the cyber area. It is in Sweden's interests that the EU strengthens its role as an actor in the area of foreign and security policy when it comes to cyber issues. The development of joint measures at EU level to respond to cyber threats and cyber attacks has given the EU a greater role as a global actor in this area. In response to the deteriorating security situation, in 2017 the EU began to develop a diplomatic toolbox with which to respond to cyber threats and cyber attacks on the EU and its Member States. The toolbox includes démarches and joint statements, support for capacity development, and an instrument for thematic sanctions. Since the sanctions regime was created in 2019, a number of cyber actors based in Russia, China and North Korea have been listed. The EU has also made a number of joint statements on malicious cyber activity, including cyber activity targeting the EU and targeting partners to the EU.

For Sweden, the toolbox provides an opportunity to act in solidarity with EU Member States and to receive support from the EU when cyber threats target Swedish interests. Sweden should continue to develop its capacity to make concrete contributions in the form of sanction proposals, for example. Furthermore, Sweden should actively support the further development of the cyber diplomacy toolbox and support the continued integration of cyber issues into the EU Common Foreign and Security Policy, while respecting that national security falls within the competence of the Member States under the Treaty on European Union. Sweden wants to see a more strategic, long-term approach to key threat actors, to strengthen the cyber sanctions regime and to develop EU cooperation in this area, including with the private sector and with NATO.

Sweden also wants to continue to develop the EU's digital diplomacy with the aim of a more strategic and coherent action on the part of the union. One way of doing this is to promote the Team Europe approach, which brings together the various EU institutions as well as the Member States. Digital diplomacy needs to be fully integrated into the EU's wider external relations. Partnerships with other democracies, especially the United States, is key in digital diplomacy.

The EU has the potential to take an even more leading role in global processes concerning norms and regulations on cyber and digital issues, not least within the UN. By virtue of the EU's internal market and regulatory power, taking into consideration how internal market policies affect other countries, the EU can take a strong position in relation to states such as China and Russia. Joint action by the EU is also essential to developing dialogue and cooperation with the United States on equal terms – in security policy matters and in matters related to data flows, storage and the regulation of digital platforms. The EU-US Trade and Technology Council (TTC) has the potential to deepen and broaden the transatlantic trade and investment relationship, avoiding new barriers to trade and cooperating on new standards and technologies. It is important to have as much agreement as possible between the EU, the United States and other democratic countries on issues related to standards and regulatory frameworks in order to prevent fragmentation of the global market from occurring, and to strengthen joint efforts on global standards and rules. The EU's regular cyber dialogue with the United States provides an opportunity to establish norms for international cyber security.

The EU today also has a growing number of structured cooperation initiatives with important countries and regional organisations that can be further developed and reinforced. This includes the trade and technology council with India, digital partnerships with countries such as Japan, Canada and South Korea, and regional cooperation, including with Latin America and the Caribbean (EU-LAC Digital Alliance).

The EU also has instruments at its disposal to assist countries with limited resources in their capacity development within the frameworks of the European neighbourhood policy and the European development policy.

Cooperation within NATO

NATO has a growing focus on strategic cyber and technology issues, linked in particular to the allies' interest in responding to challenges from Russia, but also China. NATO has extensive cooperation within the cyber defence area as well as strategic technologies.

Sweden's NATO membership brings new opportunities for strengthening Sweden's cyber defence capabilities, cyber security, cyber resilience and security at large. This also entails demands on Sweden's capacity to cooperate within the Alliance and with individual allies. NATO places great emphasis on cooperation with the innovation-driven private sector. As NATO member, Sweden wants to provide clear added value to the Alliance in these areas. Sweden's integration into NATO will also provide it with new interfaces for developing our work on innovation and new technology, as well as a platform to promote Swedish industry.

The EU and NATO should be complementary and mutually reinforcing. Sweden should work towards further enhanced cooperation between NATO and the EU, particularly in the areas of cyber defence, cyber security and cyber resilience. Unnecessary duplication between these organisations could risk impeding capacity development and should be avoided.

Nordic and Nordic-Baltic cooperation

As a complement to European and Euro-Atlantic cooperation, Sweden wants to develop foreign and security policy dialogue and cooperation between the Nordic countries. This applies to policy processes within the EU and NATO, but also to concrete security policy issues linked to the management of and response to malicious cyber threats from, for example, Russian actors. Cooperation with the Nordic and Nordic–Baltic countries should be deepened further, not least with a focus on the neighbourhood and to deepen transatlantic cooperation. Sweden will also act to support the continuing development of Nordic-Baltic cooperation in the cyber area (NB8).

Cooperation with the United States of America

There is a significant focus on cyber and technology issues in US foreign and security policy, not least as part of competition with China, and in the US management of cyber-related threats from Russia, Iran and North Korea, for example. The United States is working actively to create a global alliance of like-minded democracies on cyber and technology issues, including via the establishment of global norms, standards and regulatory frameworks. Sweden should seek to participate in US technology-related cooperation, or otherwise ensure that Swedish interests are taken into consideration. Sweden will also advocate for interoperability between EU and US positions in international processes, with a view to ensuring transatlantic and democratic leadership in the development of global digital standards and regulatory frameworks.

Cyber and technology issues are also becoming increasingly important in Sweden's bilateral relationship with the United States, in which there is a particular focus on strategic technology issues such as telecommunications, cyber security and space issues, as well as instruments for protecting new technology. Sweden has a number of bilateral agreements with the United States in the area of technology that should be used as a basis and starting point for deepened cooperation. Sweden is also engaged in a dialogue with the United States on the development of diplomatic and political instruments for managing malicious cyber threats and cyber attacks. A formal bilateral dialogu on cyber and digital issues was established in 2024.

Strategic partners

Strategic partnerships are very important to strengthening Sweden's influence in and cooperation with technologically advanced and innovation-driven democracies. Sweden will deepen its bilateral foreign policy dialogues with the United States as well as leading countries within the EU and NATO and globally, not least countries in the Indo-Pacific region.

Sweden currently cooperates with a number of strategic partners in smaller groups of countries, where the main focus is on foreign and security policy factors and responses to

malicious cyber threats. Such informal circles give Sweden the opportunity to gain insight and influence in dialogues with countries within Sweden's circle of like-minded states.

Sweden participates in a number of coalitions and cooperation forums on digital issues. One example is the Freedom Online Coalition, which consists of around 40 member states, including the United States, a number of EU countries, but also countries such as South Korea and Chile. The Coalition is an important platform for Sweden in its work with issues of rights and freedoms on the internet.

The UN and multilateral organisations

The UN has an important role to play in establishing global norms and managing cross-border challenges and risks. For Sweden, it is therefore important to safeguard and promote rules-based international cooperation and strong multilateral institutions including the UN.

Cyber security and digitalisation are addressed in multiple processes within the UN. They include the fundamental issue of how international law is to be applied, the implementation of voluntary norms of responsible state behaviour, the implementation of measures to build confidence and trust, the inclusion of civil society in decision-making, and countering systemic cyber crime. In the Open-Ended Working Group on security of and in the use of information and communications technologies work that is central to maintaining the free world order in the cyber area is being done. Sweden aims to ensure that a permanent, voluntary and open multi-party model is established as part of the international conference on cyber security to be held in 2026. Follow-up efforts on the recently adopted international convention to combat cyber crime are necessary.

In 2024, the General Assembly adopted the Global Digital Compact, a global digital framework for an open, free and secure digital future, premised on the application of international law and enabling the realisation of Agenda 2030.

The UN is also developing its work with entrepreneurship and human rights regarding new digital technologies. This includes promoting technology companies' respect for human rights both online and offline, as well as ensuring that companies exercise due diligence in their value chains.

It is welcome that the UN in general is strengthening its role in the digitalisation area in terms of harnessing the opportunities of digitalisation, ensuring that they benefit the entire population of the world, and managing the risks and challenges.

Sweden's place on the ITU's Council means that we have a solid platform for working for better standards and to ensure that the key task for developing countries – being able to become a part of the digital economy – is undertaken in a way that is transparent, effective and based on human rights and international rules and principles.

The UN has an important role to play in how international relations should be managed and developed in a digital age. But this must also be done in a way that is based on and utilises the established norms, principles and processes that exist for discussing various digitalisation issues. Generally, multi-party cooperation should characterise the UN's work on cyber and digital issues in order to harness different competences and perspectives. For Sweden, it is crucial that the governance and management of the internet at a technical level is based on the principle of multi-stakeholder cooperation that also includes the private sector.

In addition to the UN, there are other organisations that can be Sweden's partners. Sweden is a member of IDEA, which works on the link between democracy and digitalisation. The organisation has special expertise in the protection of electoral processes and institutions. Two other partner organisations, the European Endowment for Democracy and the Prague Civil Society Centre, contribute to strengthening civil society, human rights defenders and free media in the digital sphere, and promote increased participation in politics and resilience against, for example, malign information influence.

OSCE

The OSCE has adopted 16 confidence building measures in the cyber area. Among other things, a contact point system has been established in which the 57 participating States provide political and technical contact details to enable the sharing of information (for example in the event of cyber incidents). Cyber issues are discussed regularly in an informal working group. Sweden supports the OSCE's ongoing work with cyber issues. Together with other countries, Sweden has undertaken to pursue and develop the confidence building measure concerning public-private partnerships.

World Bank

The World Bank Group and the regional development banks are now strengthening their support to digital development and the digital transformation of partner countries through capacity development, policy dialogue and investment in technological and digital infrastructure. For Sweden, it is important to ensure that digital economic development within the framework of the World Bank Group includes a cyber security perspective, and to promote digitalisation's potential to contribute to achieving the 2030 Agenda. Sweden wants to strengthen the World Bank Group's work on integrating cyber and digital issues within the Bank, and also into its partnerships and strategies. This is all the more urgent in light of the necessary reforms facing the World Bank Group.

Focus areas – international cooperation forum

- Promote the EU's capacity to act as a coherent foreign policy actor on cyber and digital issues. Contribute to coordination between the EU's cyber diplomacy and digital diplomacy. Continue to develop the EU's capabilities to prevent, manage and respond to

cyber threats and cyber attacks using foreign policy and diplomatic means, with a focus on the development of the EU Cyber Diplomacy Toolbox.

- Establish Sweden as a foreign and security policy actor in NATO's ongoing projects and processes in the technology, innovation and cyber areas, with the objective of explicitly adding value to the Alliance and to Sweden.
- Develop Nordic and Nordic-Baltic cyber cooperation in the digital area, and with other strategic partners.
- Develop the formal bilateral dialogue with the United States on cyber and digital issues, and enhance the broader cooperation on strategic technologies.
- Develop Sweden's partnerships with selected like-minded states on deterrence in the cyber area.
- Work for closer EU-US cooperation within the framework of the TTC and other relevant forums to ensure transatlantic leadership in the development of international norms and standards.
- Develop Sweden's, the EU's and NATO's partnerships concerning support to Ukraine in the cyber and digitalisation area.
- Actively participate in the UN's policy development and negotiations in the cyber and digitalisation area with a focus on the application of international law, the development and implementation of norms and measures to build confidence and trust. Work within the UN to ensure that multi-stakeholder participation in general will characterise this work. Defend the internet governance model based on multi-stakeholder participation. .
- Safeguard Sweden's and the EU's interests and values within the framework of the implementation of the UN's Roadmap for Digital Cooperation, as well as the UN's Global Digital Compact.