White paper

Cisco

Accelerating Europe's Digital Transformation

Digital Priorities 2019-2024

Cisco is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity, today.

Introduction: A parliamentary term at a time of change

The next European Parliament and Commission are taking up their office at a time when digitisation taking off and when technology will impact every aspect of our lives.

This can be seen by the exponential growth in IP traffic and explosion in devices as everything is being connected. In the next five years, IP traffic will grow threefold, equivalent to every film ever made crossing European networks every 6 minutes.[1] As virtually all EU citizens are already connected today, this traffic growth shows digitisation is taking hold with more than half of the 5.1 billion connected devices in 2022 being Machine to Machine (M2M) devices, bringing everything from our homes to our cities, cars and our workplaces, online.[2+3]

Consequently, this term will be an opportunity to make sure digitisation is delivering true value for citizens and societies and happens in an inclusive and secured manner. Cisco believes there are four key areas where further action is needed in the next term to underpin a digital transformation that creates societal value and economic growth.

Creating a dynamic and innovative single market for digitisation

We need an overall regulatory framework for businesses that fosters innovation and investment in digitisation in the single market. As Cisco's research on digital readiness shows, ease of doing business is an important driver for an economy's readiness for digital transformation.[4] Businesses in Europe need a renewed focus on the single market, rules that are harmonised, follow a 'comply once' principle and that distinguishes between the business and consumer markets (B2B and B2C).

Building ubiquitous and secure high capacity networks & creating trusted communications

To enable digital transformation, Europe needs to maintain a laser sharp focus on deploying ubiquitous high capacity and secure digital infrastructures capable of supporting the phenomenal increase in connected devices across all segments of society. As more and more devices are connected, the threat surface and the potential for cyber-attacks increase. This makes it imperative to secure digital networks and services end to end. Only when users will trust the safety of their communications can we truly unlock the potential of digital transformation.

In this regard, important progress has been made in the previous term with the adoption of the European Electronic Communications Code (EECC), the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS). Further work on all these issues will be needed in the next term, both in terms of implementation and new initiatives to complement these already agreed measures.

A Europe that innovates and enables a globally competitive digital industry

Several policies impact Europe's ability to innovate. There are however three key points as regards digital innovation where we believe the next Parliament and Commission should focus. Firstly, digitisation can be driven equally by the public sector as the private sector. To enable this, public procurement needs to focus more on innovation and quality rather than lowest price. Secondly, as public and private sector are digitising they will be relying on connectivity standards which traditionally have been contained to the ICT sector. As this is happening, it becomes ever more important to ensure that the IPR licensing for such standards occurs on fair, reasonable and non-discriminatory terms. Finally, in order for Europe's digital industry to compete globally and Europe's businesses and consumers to have access to the best in class technology, the next Parliament and Commission should maintain its focus on enabling digital trade and create a level playing field.

Transforming in an inclusive, ethical and sustainable manner

Last but not least, we need to make sure the digital transformation happens in an ethical, inclusive and sustainable manner. In order to ensure Europe excels at AI and can use technology to drive societal value, digital skills need to remain centre stage. This means doubling current efforts to improve European citizens' digital skills and increasing the proportion of women in the digital sector. It also means using digital technologies to help us reach our sustainability targets and foster the circular economy.

Below we set out in further detail the initiatives Cisco believes the next European Commission and European Parliament should prioritise to enable Europe to take a digital leap forward in the next five years and beyond.

[1] Total European IP traffic will grow from 22.5 exabytes (EB) per month in 2017 to 63.6 EB per month by 2022.
[2] In Europe, the connected home will be the largest segment followed by connected work. The fastest growing vertical is smart city at 31% CAGR, followed by connected cars (28% CAGR) and health (26% CAGR).
[3] All data in this paragraph is from Cisco's Visual Networking Index 2017-2022, available here. European numbers are calculated by adding Western Europe and Central & Eastern Europe values minus Russia.
[4] https://www.cisco.com/c/dam/assets/csr/pdf/Country-Digital-Readiness-White-Paper-US.pdf

Creating a dynamic and innovative single market for digitisation

Cisco's research on digital readiness shows that ease of doing business is an equally important determinant for enabling digitisation as e.g. skills and digital infrastructures.[5] If we want the European economy to digitise, we need a general regulatory environment that promotes ease of doing business.

This firstly means more, not less, single market. The next European Commission and Parliament should therefore always aim for the highest level of harmonisation. Harmonisation does not and should not come at the expense of the necessary level of protection. It is simply a call for **'comply once'** which will be to the benefit of consumers and business alike. Policy-makers need to recognise that Europe will continue to have a scale-up problem as long as doing business in Europe requires being familiar and compliant with 28 variants of EU single market law. One important example of this is the EECC which, as a Directive, will not deliver the kind of genuine single market needed for today's digital communication services.

Secondly, a distinction needs to be drawn between the business and consumer markets. In policy discussions around emerging technology such as 'platforms', Artificial Intelligence (AI) and the data economy, we are observing a blurring in the debate between the B2C and B2B markets. As policy discussions evolve from the general to the concrete level, increasingly they do not further refine the markets in which the policy concerns arise. This is a concerning trend considering the significant differences that remain between these markets. **In the B2B market, contractual freedom should remain the core principle** and policy-makers should only deviate from this in case of strong evidence of systemic market failure in well-defined and scoped markets.

This would equally help prevent the cases where online business platforms get caught in legislation aimed at consumer platforms because some of these services may appear similar at first glance but in fact from a tech and market perspective differ.

Policy Recommendations:

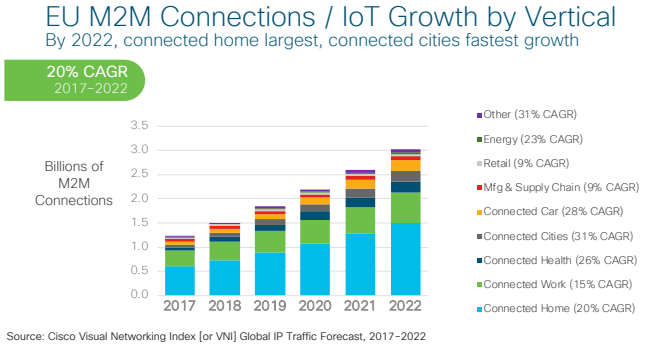
- Harmonise to the largest possible extent to tackle fragmentation across the EU and implement the 'comply once' principle.
- Distinguish between B2C and B2B as significant differences in these markets require a different policy response.

[5] https://www.cisco.com/c/dam/assets/csr/pdf/Country-Digital-Readiness-White-Paper-US.pdf

Building 5G and ubiquitous high capacity networks for digital services of the future

Traffic demands and status quo of network deployment

The ubiquitous availability of secure high capacity digital infrastructure, including 5G, is fundamental to enable the digital transformation and to meet the traffic requirements of a fully connected society and economy. Not only will our future networks need to overall carry a lot more traffic, they will also need to be able to cater to a much more heterogenous mix of applications, notably with 60% of devices being M2M in 2022. Some of these will require quality of service parameters such as low latency without having too high bandwidth requirements and others, increasingly, will require both low latency and high bandwidth, e.g. live video increasing from 5% to 17% by 2022, and virtual & augmented reality which is set to increase 12-fold.[6]



Source: Cisco Visual Networking Index [or VNI] Global IP Traffic Forecast, 2017-2022

Europe is partly on track in deploying these high capacity networks with speeds set to increase for both fixed, mobile and Wi-Fi networks[7] and 5G commercial deployment set to begin with 13.1% of mobile traffic in Europe expected to come from 5G by 2022.

However, when comparing this progress to the EU target of 100% coverage of 100Mbps by 2025[8] and to Europe's global peers, Europe is still lagging behind.[9] Fixed speeds are set to increase to 98.4Mbps in Asia Pacific and 94.2Mbps in North America and 5G will account for 41.1% of mobile traffic in Japan, 38.8% in the US and 35.6% in Korea by 2022.[10]

5G: the next generation of end-to-end networking

5G is much more than the next generation of radio cellular technology. It is the next generation of networking, from the core network that connects to and powers the internet, the transport layer that turns radio data into internet protocols and the radio access networks (RAN) made up of cell towers, and the devices that connect to those towers using custom mobile chips.

The socio-economic promise of 5G as the driver of digitisation, not just faster consumer mobile broadband, will only be delivered if 5G is understood and implemented as this wholesale transformation of mobile networks, not just a RAN upgrade.

The policies impacting 5G rollout therefore also expand beyond spectrum though the timely availability of spectrum remains a sine non-qua for 5G rollout.

[6] Cisco VNI, global numbers.
[7] Speeds will increase from 35.5Mbps in 2017 to 68.4Mbps by 2022 for fixed networks and 14.3Mbps to 41.4Mbps for mobile networks. Wi-Fi speeds will also improve from 23.1Mbps to 44.6Mbps.
[8] EU 2025 connectivity targets: 100% availability of at least 100Mbps for all citizens; 1GB for 'socioeconomic driver sectors'; 5G in all urban areas and major roads and railways, starting with commercial service in at least one major city in each EU member state already by 2020
[9] The European average covers large regional divergences with some European countries being amongst the global leaders, e.g. Sweden with 34.7% 5G traffic by 2022 and e.g. Spain with fixed speeds at 115.2Mbps by 2022.
[10] Cisco VNI 2017-2022 and Mobile VNI 2017-2022

On a whole, Europe's 5G policy should have two goals in mind. One is how **to lower costs and increase incentives for network deployment** and the other is how to ensure that, once built, operators have sufficient **commercial freedom to use these networks to offer a much wider set of services and applications tailored to the needs of different customer segments and individual users.** Regulation has to be based on the fact that business as usual, and business models as usual, will not ensure a sufficient return on investment and therefore will not unlock the full potential of 5G.

Investment-friendly implementation of the Code

Whether we are talking about 5G or fixed networks, the European Electronic Communications Code ('the Code) adopted in 2018 rightly aims to bridge the connectivity gap and contains new tools to incentivise network investments. However, Member States and national regulators have significant discretion how and whether to use these tools. **It is therefore crucial that the Code is implemented in a consistent manner across Member States in line with the spirit and objective of the reform to incentivise investment and provide longer term certainty to the market.** This in particular needs to be reflected in the BEREC guidelines on co-investments in Very High Capacity Networks (VHCNs). The implementation should look to use the tools to increasingly shift the focus on access to civil engineering as this represents the greatest possibilities to reduce network deployment costs, thereby fostering infrastructure-based competition. This includes taking full advantage of the Broadband Cost Reduction Directive.

Policy-makers and regulators also need to **focus special attention on ensuring connectivity to all rural parts of Europe** with currently only 47% of citizens having access to broadband speeds of 30Mbps and only 10% to 100Mbps.[11]

The next European Parliament needs to stand firm on the proposed funding levels for digital infrastructures in the next Multiannual Financial Framework of €3B for digital in the Connected Europe Facility; €9.2B for Digital Europe and funding for digital projects under the European Regional Development Fund. Finally, the European Commission should also **review the state aid guidelines** to bring them in line with the 2025 connectivity targets and broadband mapping and digital exclusion areas under the Code.

More spectrum for 5G and Wi-Fi

The next Commission and Parliament need to continue their support for more spectrum harmonisation. Considering in future 5G/4G/Wi-Fi/unlicensed LTE will work together, we need more licensed as well as unlicensed spectrum in low (below 3 GHz), mid-band (3-24 GHz) and high band (above 24 GHz).

More spectrum for unlicensed is particularly important to ensure users will be able to fully benefit from the new capabilities of Wi-Fi 6. With the new Wi-Fi 6 standard, Wi-Fi will be an important complement to 5G cellular radio as Wi-Fi6 will be able to support deterministic networking and low latency similar to 5G cellular radio and can be placed where users need them to provide better geographical coverage at a lower cost. Wi-Fi will carry 55% of total European IP traffic by 2022 and more traffic will be offloaded onto Wi-Fi networks from mobile devices than will stay on mobile (cellular) networks. Globally, Wi-Fi contributed $1.96 trillion in economic value in 2018, growing to $3.47 in 2023.[12] **Cisco fully supports the work underway to open up 5925- 6425 MHz in Europe and is hopeful that a decision can be taken in 2020.**

[11] European Commission Digital Economy & Society Index 2018, Connectivity report available here
[12] The Economic Value of Wi-Fi: A Global View (2018 and 2023), October 2018, available for free download at the Wi-Fi Alliance website, www.wi-fi.org.

Regulators also need to ensure a European harmonised approach to lightly licensed spectrum for industrial use (operated by the business itself or by an operator). Germany has taken the lead within Europe to designate 3.7-3.8 GHz for industrial use and other European regulators are exploring the issue. We support this work and would encourage European regulators to develop a shared approach. We also believe Europe should support that part of the millimetre wave band scheduled to be allocated at the 2019 World Radio Congress should equally be considered for industrial use.

Finally, policy-makers and regulators need to **ensure access to rights of way and the least onerous administrative procedures and requirements for deployment of small cells.** The European Commission implementing act for this provision in the Electronic Communications Code ('the Code') needs to harmonise such requirements to ensure that deployments can proceed under reasonable terms and conditions that are both transparent and predictable.

Net neutrality conducive to innovation

Cisco continues to believe the EU Net Neutrality rules are overall fit for purpose from the perspective of protecting consumers of Internet Access Services (IAS) from blocking and anti-competitive practices whilst ensuring operators together with app and other service providers are free to innovate in new quality managed services.[13]

However, **the current BEREC guidelines and certain national enforcement create uncertainty that some regulators impose additional conditions above and beyond the Regulation** that risks leading to the regulator, not the customer, deciding if there is a need for a specific level of quality. We do not believe this is in line with the Regulation and we believe it would significantly hamper the innovation potential in Europe for 5G considering the greatest potential of 5G lies in the ability to offer services specific to the individual user's quality of service requirements. It is in this regard also relevant to distinguish between the consumer and enterprise markets. **The BEREC guidelines therefore need to be changed to make sure the application of the Regulation stays true to its intent and that there is 'no permission to innovate' in the 5G era.**[14]

Policy Recommendation:

- Ensure the Code is implemented in a consistent manner that fosters investment.
- Maintain proposed funding levels for digital infrastructures and rural connectivity.
- Free up the 6GHz spectrum band for Wi-Fi.
- Create a harmonised European approach to lightly licensed spectrum for industrial use.
- Amend BEREC's Net Neutrality guidelines to ensure there is no permission to innovate in the 5G era.

[13] These services are often referred to as 'specialised services' but they are purposefully not defined in the Regulation to keep it open which services can be delivered with SLA. Hence, they are called Services other than Internet Access services.
[14] For further details: https://emear.thecisconetwork.com/site/content/lang/en/id/8910

Trust, Privacy & Security

Trust: A prerequisite for digitization

Trust is a prerequisite for successful digital transformation. Users need to trust that companies processing data about us are responsible data stewards and are acting on data in a way that aligns with our expectations. We have to trust that malicious actors are not able to affect the confidentiality, integrity or availability of sensitive data of businesses or individuals. And we need to trust that the infrastructure underlying critical business operations will not be disrupted in a way that will impact our economy and society.

Trust should not be blind: it should be verifiable. Companies need to be transparent about how they embed privacy and security into their people, processes and technology. They need to be able to demonstrate that they live up to their promises, and to be held accountable for meeting them.

Implementing the data protection framework

The General Data Protection regulation (GDPR) is a success story for Europe. The legal framework for data protection has a long history reaching back through the fundamental rights established in the post-war period, the OECD Principles of 1980 and the EU's Data Protection Directive of 1995. The GDPR has reinforced Europe as the global thought leader in this arena. The rest of the world is taking note. In a survey of more than 3000 companies across the world, Cisco found that only 4% of companies outside the EU believed the GDPR did not apply to them and 86% were either GDPR ready or believed they would be within a year.[15]

Fundamentally, we believe that data privacy is good for business. It is about putting the individual at the centre of the debate.

Being transparent in how their data is being used, giving them control over how their data is being used and ensuring that organisations are accountable for managing their data. To do that, organisations need to know their data really well. The side effects of doing that right are shorter sales delays; fewer, smaller and less costly data breaches and increased agility and innovation.[16]

With the world watching, there are two aspects the EU needs to get right in the coming term.

The first is about setting the right priorities for implementation. Data Protection Authorities (DPAs), and the European Data Protection Board (EDPB) which gathers them together, need to **focus on creating a privacy culture within organisations under their jurisdiction.** Data protection is not something organisations should only be tagging on at the end by asking individuals to consent to a legalistic privacy policy.

[15] Cisco 2019 Data Privacy Benchmark Study, available here.
[16] Average sales delays due to customer privacy concerns are 2 weeks less for most GDPR-ready companies versus least; EU companies reported average breach size of 74,000 records for most GDPR-ready versus 160,000 for least and 39% reported greater agility and innovation as an advantage of privacy practices. Ibid.

It is something they should be building in to products and services from the ground up. DPAs should take inspiration from the UK's ICO regulatory sandbox, enabling joint understanding of compliance[17]; promote certifications that build-in privacy culture like the BCRs[18]; leverage industry Codes of Conduct[19] such as the EU Cloud Code of Conduct and continue to seek industry input into the EDPB Guidelines on GDPR implementation. **The European Commission needs to plug a gap in existing mechanisms for transferring personal data outside the EU.** Specifically, develop standard contractual clauses for an EU data processor to transfer data to another processor outside the EU.

The second aspect is about the EU's role in the world. More than 130 countries have comprehensive data protection laws in place and many are currently adopting or revising laws. As a global leader, the European Commission should continue to **advise countries in the adoption of their privacy frameworks.** In our experience, while there are many details that make for a successful law, three stand out: **scalable means of data transfer, suitable grounds for data processing and workable data breach notification.**

The EU should look to take the lead in developing multilateral mechanisms that will rationalise the current bilateral or single jurisdiction approach while ensuring the same standards of protection. They should also seek to push back on countries who want to use data protection as an excuse to insist on data localisation, such that the data cannot leave their borders. Many countries fall back on consent as the primary or sole means to legitimately collect and process data. The EU should look to explain how and why it has adopted a broader range of grounds for processing data. Finally, the EU should encourage countries to differentiate between significant and minor breaches and to allow companies to implement a timely and effective process for investigation and notification.

ePrivacy

The GDPR called for the ePrivacy Directive (ePR) to be reviewed to ensure its consistency with the general data protection framework.[20] The draft ePR seeks to set out rules that protect the rights of natural and legal persons in the provision and use of electronic communication services. As such, with the realm of electronic communications, it applies to both personal data and non-personal data, to both individuals and legal entities.

Unfortunately, **there is a fundamental difference in approach between the ePR and GDPR, which calls into question the former's suitability as currently crafted to ensure consistency between the two.** The GDPR has three basic classes of data which are subject to additional layers of protection as one moves up the stack: non-personal (or anonymous) data, personal data and special categories of personal data (or sensitive data). Entities processing the data have an incentive to work with the least sensitive category possible, for example by anonymising their data sets.

In the ePR, from a risk perspective there is a fairly arbitrary distinction between metadata, content data, data on devices, processing capabilities of devices and network/device connection data. For certain types of data, there is a limited range of grounds for processing and an overreliance on notice and consent. For example, a traffic management system that uses data from connected cars and roadside infrastructure to inform road-users and manage traffic could legitimately process data under GDPR, using a combination of legal grounds such as public safety or vital interests of the data subject. With a lack of means to obtain consent from the end user, under ePR it has no legal grounds to operate. The risk is that the ePR could cannibalise the GDPR insofar as communication is central to modern data processing activities, and it applies across industry sectors and public sector environments like smart cities.

[17] ICO Regulatory Sandbox
[18] EU Binding Corporate Rules
[19] EU Cloud Code of Conduct
[20] Recital 172, Regulation (EU) 2016/679

The Commission actually suggests an appropriate way forward in the Explanatory Memorandum of the ePR. It states that it intends to evaluate whether a separate legal act remains necessary in light of legal, technical and economic developments and taking into account the first evaluation of the GDPR, due by 25 May 2020.[21]

As such, **we recommend that the EU institutions withdraw the current proposal and take the opportunity of the review in May 2020 to rationalise the structure and enable true consistency with GDPR.** A single article could extend the right to confidentiality across all electronic communications data, not just personal, with Article 6 of GDPR standing as the reference point for legal grounds for processing such data.

Government handing of vulnerabilities

Governments in the EU and beyond should **put in place clear policies relating to the handling and disclosure of security vulnerabilities.** Some governments are researching, developing, purchasing, and licensing zero-day vulnerabilities and their exploits.[22] However, this should not be done without sufficient safeguards, including due process for their handing, retention, use or disclosure.

The US has had a Vulnerabilities Equities Process (VEP) since 2010, which was updated in 2017 with the VEP Charter. In Europe, activities have been more sporadic. The UK's GCHQ has led the way by adopting a VEP process in November 2018. **There has been a lack of coordinated debate on the topic in Europe, however, and we believe the EU could play a vital role in helping Member States establish the rules of the game.**

The decision on whether to retain or disclose vulnerabilities should not be binary. **It should not be a matter of 'if' governments are required to notify vendors, but 'how long' until governments must notify them.** Rules should be designed to quickly route information about vulnerabilities to organisations capable of acting upon it to protect security in a timely manner. Retained vulnerabilities must be subject to periodic review, with the potential economic, reputational and social damage to companies and individuals taken into consideration.

Vendors are also responsible. It is incumbent upon industry to demonstrate that vulnerabilities disclosed to them are treated in a risk-based way with regard to when and how they are patched. Vendors should have a publicly disclosed and standards-compliant mechanism for communicating how they receive vulnerability information, how it will be used, and how patches, mitigations, or work-arounds will be communicated to their customers and downstream users.

[21] Section 5.2, Explanatory Memorandum, ePrivacy Regulation proposal, 2017/003 (COD)
[22] Exploits are techniques or actions that can be used to take advantage of vulnerabilities. Where such vulnerabilities are not known to the vendor or the public at large, they are generally referred to as zero-day vulnerabilities.

EU-US bilateral on access to data by law enforcement authorities

Over the last few decades, law enforcement authorities (LEAs) have become increasingly interested in electronic evidence, supplementing physical evidence in criminal investigations. In a world where international data flows are the norm, the data may be subject to laws of multiple jurisdictions. This can put companies in a position where they must choose between complying with law requiring them to hand over data for evidence purposes in one country or law in another that forbids them from handing over the data to protect rights such as protection of data.

While there are efforts to reform the Mutual Legal Assistance Treaty (MLAT) process, **both the EU and the US consider it necessary to enable LEAs to make demands direct to tech companies,** regardless of location of data, in order to make certain demands more efficient.

The US CLOUD Act clarifies that US LEAs may lawfully demand certain data stored in foreign countries from entities subject to their jurisdiction. The draft EU e-Evidence Regulation proposes that data may be demanded regardless of its location.

We recognise that LEAs needs for direct demands to access data but believe it **should be subject to a government-to-government framework that provides legal certainty for entities from which the data is sought and creates safeguards** that introduce transparency and protect the fundamental rights of the individuals to whom the data relates.

The Member States provided the Commission with a negotiating mandate to enter talks with the US in June 2019. **Cisco calls on the EU institutions to adopt a version of the e-Evidence Regulation that implements the necessary safeguards and for both the EU and US authorities to prioritise the conclusion of a bilateral deal.**

Policy Recommendation:

- Implement the GDPR in a manner that creates a privacy culture in organisations under their jurisdiction.
- Plug a gap in existing mechanisms for transferring personal data outside the EU and take the lead in developing multilateral mechanisms for data transfers.
- Advise 3rd countries adopting or revising their data protection laws and lead the path to multilateral data transfer solutions.
- Use the opportunity of the first review of the GDPR to reset the proposed ePrivacy Regulation.
- Lead the European debate on government use of security vulnerabilities.
- Adopt an eEvidence Regulation with appropriate safeguards and reach an EU-US bilateral agreement on access to data by law enforcement.

[23] GCHQ Equities Process
[24] Negotiations on 2nd Additional Protocol to the Budapest Convention. See European Commission's FAQ for further information.

A Europe that innovates and enables a globally competitive digital industry

Public procurement that drives innovation through quality and security

The public sector is digitising just like the private sector. Public procurement plays a large role in this transformation with more than 250,000 public authorities in the EU spending around 14% of GDP on the purchase of services, works and supplies each year. To ensure public procurement drives digitisation, the focus needs to shift away from lowest cost and increasingly focus on innovation and quality. **We urge the next Commission to develop guidance on how contracting authorities can include criteria such as innovation, quality, customer service, social responsibility and security in their award criteria in order that the 'Most Economically Advantageous Tender' (MEAT) is not determined by lowest price alone.**

Further, to advance secure digital public services, additional guidance is also needed on how to integrate cyber security considerations in tenders. Both could be done in the form of a handbook as exists for instance for green procurement and through sharing best case practice in the Central Purchasing Bodies (CPBs) Public Procurement Network.

IPR licensing that unlocks the IoT potential

Many innovations in the area of Internet of Things (IoT) will rely on connectivity standards to allow devices to communicate with each other. In order to unlock the potential growth and innovation in Europe based on the development of IoT, it is crucial that the large amount of IoT developers are able to get licenses to the underlying standardised technologies (Standard Essential Patents, SEPs) on fair, reasonable and non-discriminatory terms and at all levels of the value chain. This in line with the commitments that SEP owners have provided to Standards Bodies prior to the inclusion of their technologies into the standard. The European Commission and Parliament should therefore foster an environment in which these commitments are respected.

Enabling innovation through digital trade

To reap the full potential of digitisation, Europe should take the lead in creating new rules of the road that **enable digital trade and that address distortive practices and new 'behind the border' barriers.** The next Commission and Parliament should also **focus on enforcement** to ensure trade happens on free and fair terms and that countries respect the commitments they themselves have entered into.

The Transatlantic relationship should in this regard be maintained and strengthened. Cisco remains committed to Europe and believes that there is much more which unites the US and Europe.

[25] https://ec.europa.eu/growth/single-market/public-procurement_en

We firmly believe both economies are stronger when working together and hope current tensions can be resolved as soon as possible in order that the new Commission and Parliament can focus their efforts on leveraging a strong Transatlantic partnership to **address global trade challenges, distortive trade practices and new forms of digital protectionism.** We urgently need new disciplines on forced disclosure of source code or other technology as well as forced localisation and local content requirements, e.g. for manufacturing or local infrastructure. We urge the Commission to pursue these priorities in future bilateral agreements as well as the multilateral level, in particular in the ongoing e-commerce negotiations. It is also crucial to ensure the **WTO Moratorium on Customs Duties on Electronic Transmissions is renewed.**

The global competitiveness of European industry is not only determined by the opportunities created by EU's trade agreements. For the ICT industry the EU's rules on export controls of dual-use items play a significant role in enabling EU exporters to easily serve their global customers without delays etc. **The EU Export Control Regulation** generally functions well, providing a clear set of rules for items that require licences and sits firmly within the international agreement, Wassenaar, which regulates these items on a global level. **We welcome the Member States' position on the reform and we hope the upcoming trialogue negotiations will work to make sure the new rules continue to follow the international regime whilst addressing the political objective to promote human rights.**

Policy Recommendation:

- Develop guidelines on 'MEAT' to ensure public tenders are not awarded on price alone and cyber security considerations are integrated into contract criteria.
- Ensure IPR licensing for connectivity standards occur on fair, reasonable and non-discriminatory terms.
- Maintain and strengthen the Transatlantic relationship to address global challenges of digital protectionism and distortive trade practices.
- Prioritise digital trade chapters in all future agreements at bilateral and multilateral level, incl. an ambitious WTO e-commerce agreement and extension of the moratorium on custom duties on electronic transmissions.
- Reform the EU Export Control Regulation in a manner consistent with the international regime.

A digital transformation that fosters an ethical use of technology and an inclusive and sustainable economy & society

Artificial Intelligence

Artificial intelligence and machine learning promise huge potential. These technologies are already being seen in homes and businesses alike and will certainly play an ever-greater role in the years ahead and, if managed well, could lead to huge advances in innovation, productivity, efficiency and customer services. Cisco for instance uses AI across our portfolio from making our collaboration tools more interactive to managing networks more effectively and spotting or blocking cyber threats.

At the same time as offering huge potential, we recognise some applications of the technology may give rise to concerns. Considering the still relatively early stage of development and the breadth of applications across different industries, we believe policy-makers need to address these questions step by step and in collaboration with researchers and businesses to help steer the AI opportunity in the right direction.

Appropriate time should now be given for the piloting phase of the draft EU ethics guidelines with further evaluation work happening in close consultation with industry.

This work should also include working with international stakeholders and governments from around the world to ensure a convergence of principles amongst likeminded countries.

Europe should also **maintain a focus on investment and approve the proposed increase in funding for AI research and deployment projects** in the Horizon Europe and Digital Europe programmes. These programmes should happen in close collaboration between industry and academia and to create synergies with national projects. This also includes work on skills. It is clear that AI will have an impact on jobs. A recent study by Cisco and Oxford Economics forecasts that 6.5 million US jobs will either be disrupted or displaced as a result of AI in the next 10 years. **Governments and businesses should work together to ensure training schemes, such as Cisco's Networking Academy, are made available to people looking to develop digital skills either at the start or throughout their careers.**

Policy Recommendation:

- Give sufficient time to the pilot phase of the ethics guidelines and maintain the public-private partnership between industry, international stakeholders and governments on their further development.
- Approve increased funding levels for AI research and deployment projects under the Horizon Europe and Digital Europe programmes.
- Continue working with industry to ensure the re- and upskilling of workers impacted by AI.

[21] Section 5.2, Explanatory Memorandum, ePrivacy Regulation proposal, 2017/003 (COD)

Digital skills

Cisco is fully committed to help address the digital skills gap in Europe. Since inception in 1997, our now almost 3000 Networking Academies have trained 2.2 million students including over 400.000 Cisco certified ready students (IT-Professionals) and contributed €800M in kind to education. We participate in the European Commission's Digital Skills and Jobs Coalition where we have submitted a number of key pledges: to train at least 1 million more students over the next five years, to expand our curricula to include Industry 4.0 courses, to create a competence and job-matching system and finally to provide Professional Digital Skills training for Refugees. We are also working closely with several national security initiatives and the European Cyber Security Month campaign to increase cyber security training with a new Networking Academy cyber security courses.[26]

We also firmly believe in efforts to encourage more girls to choose a career within IT and technology with initiatives such as Greenlight 4 Girls[27] and Girls Power Tech[28] as well as promoting diversity and equal opportunities within Cisco.

During the next term we recommend to **continue work on the "e-Skills Quality Label Project"** to measure global industry standard certifications against the European e-Competence Framework (e-CF).[29] This would be an important step to make competence levels transferable and recognised in all Member States and provides transparency for learners and employers.

We also recommend to **increase collaboration with national ministries of education to introduce basic competences in cybersecurity** on every education level. European programmes for adult education and retraining should also include basic competences in cyber security.

Policy Recommendation:

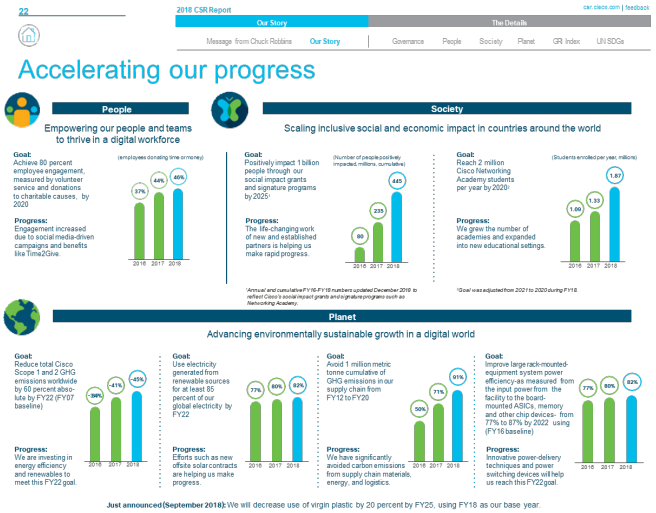
- Work to establish an 'e-Skills Quality Label'.
- Increase collaboration with national education ministries to introduce basic cyber security training at all levels of education.

[26] For an overview of the cyber security online-course offers see https://www.netacad.com/courses/security
[27] http://greenlightforgirls.org/cisco
[28] https://www.cisco.com/c/en/us/about/csr/stories/girls-power-tech.html
[29] For reference see: http://www.eskills-quality.eu/home.html

Sustainability

The circular economy principle is fundamental to how Cisco does business. Our holistic approach extends from how we design, build, and deliver products and solutions, to how we value the assets we have and turn those assets into new products.

We are also applying Cisco technology to support our customers through their own circular transformations. 82% of our global electricity use came from renewable sources and we have achieved a 45% drop in greenhouse gas emissions (compared to our fiscal year 2007 baseline) and collected 129 metric ton of used electronics at Recycle IT Day 2018.



We welcome efforts under the previous term to encourage the transition to a circular economy and believe such efforts should be continued by the next Commission and Parliament. In doing so they should distinguish between the consumer and business markets. This is for instance crucial in the discussion around the right to repair. In the ICT market, product and spare part repairs, e.g. core routers, large networking equipment or data centre servers, are done in an entirely different way than for ICT consumer goods. Such repairs are done by dedicated specialised staff under contract for and trained by the manufacturer.

Introducing a right to repair for independent local repairers outside of contract with the manufacturer is not advised because of issues with safety (high voltage/current), IPR and technical difficulties to repair. It is furthermore not necessary for circular economy purposes as any product or spare part being repaired is a highly valuable asset for the manufacturer which is circulated within a fully closed loop that always remains under the control of the manufacturer. The risk of such goods and spare parts ending up in land waste is therefore virtually non-existent. For these reasons it is also crucial to create better conditions for the cross-border flow of used products while protecting against illegal practices.

Policy Recommendation:

- Encouraging the circular economy while bearing in mind the differences between the B2C and B2B markets, limiting any potential new right to repair to consumer goods and ensuring the free flow of repaired goods and spare parts.