The European Union's digital assertiveness

Bendiek, Annegret; Berlich, Christoph; Metzger, Tobias

Veröffentlichungsversion / Published Version
Stellungnahme / comment

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

SWP Comments

Stiftung
Wissenschaft und
Politik

German Institute
for International and
Security Affairs

The European Union's Digital Assertiveness

Annegret Bendiek, Christoph Berlich and Tobias Metzger

The European institutions and EU member states are pushing hard for closer digital integration. In view of the diverse challenges – from protecting critical infrastructure and safeguarding civil liberties to the creation of common markets – "positive integration", that is targeted EU regulatory action, is the way to tackle market failure within and beyond Europe. Draft regulations at the EU level are to take effect inside and outside the internal market: the Digital Single Market Strategy (DSM), the General Data Protection Regulation (GDPR) and the Directive on Network and Information Security (NIS). Digital integration is a precondition for establishing European standards and norms effectively, especially in international politics.

Digital information systems, above all the Internet, play a central role in the free movement of goods, services and people across borders. Legislation at all levels struggles to keep pace with rapid technological advances, leaving many areas inadequately regulated. Yet legal security in dealing with technology and lasting public confidence in its reliability are crucial to economic development. For its current five-year term, the European Commission estimates that creating an interconnected digital single market could create additional growth of up to €250 billion.

Following the concept of negative and positive integration (Fritz W. Scharpf) there are two main options for state (de-)regulation in response to an expansion of economic space beyond national borders. Negative integration removes obstacles to competition and free trade (such as tariffs). This has a market-creating effect. Positive integration measures aim to correct market outcomes and overcome market failure. This requires economic policy coordination and regulatory powers at the EU level. Therefore, digital integration – analogously to previous non-digital economic integration – should be understood as the expansion of a unified societal space, which is subject to shared rules and which is characterised by the removal of institutional barriers between EU member states. Fundamentally, market regulation happens at multiple levels: global standards must be set in international forums, data protection should be harmonised at the EU level, while prosecution of cybercrime is mostly done at

Dr. Annegret Bendiek is a Senior Associate in SWP's EU/Europe Division
Christoph Berlich and Tobias Metzger are SWP Project Assistants on »The challenges of digitalization for German Foreign and Security Policy«

the national level (if necessary coordinated EU-wide). Digital regulation should, therefore, be understood as a multi-layered structure. The existence of the single market makes the Union not only an important locus of regulation, but also a strong economic actor with the global ambition of digital assertiveness. In the past, establishing standards such as MP3, SMS and Compact Disk in Europe has proven effective in compelling non-European market participants to join. As the experience of Airbus has, and the satellite navigation system Galileo might, demonstrate, the EU framework can enable state and non-state actors to influence global standard-setting to an extent denied to individual states and private corporations.

Challenges of the Digital Single Market

The challenges associated with creating a digital single market can be illustrated by the virtual path of an e-mail. Which 1) hardware and software is used to write an e-mail, via which 2) Internet routing infrastructures is it transmitted, on whose 3) data servers and cloud services is it saved, with which 4) techniques is it encrypted there, and by which 5) data protection and competition regulations is it protected? These steps along the digital path demonstrate the need for regulation and reveal why the European Union is the appropriate level at which this should occur:

Firstly, Europe, apart from a handful of exceptions such as SAP and Alcatel-Lucent, has ceased to be a relevant actor in the software and hardware sectors. The European industry's dependency on US and Chinese components makes a completely independent European market inconceivable. Many industries, such as that of search engine providers, are currently dominated by quasi-monopolists: Microsoft, Google, Cisco and Huawei. The leading PC manufacturers include Apple, Dell, HP (all USA), MSI, ASUS, Acer (all Taiwan), Samsung (South Korea), Lenovo (China) and Toshiba (Japan). Some of these are also among the world's leading smartphone manufacturers, alongside Huawei (China) and LG (South Korea). Hardware components for home networks originate largely from Cisco (USA) or Huawei (China), while HP leads Dell and IBM in server hardware for data centres. The market share of European competitors (Siemens, Nokia) has shrunk significantly, leaving a de facto US-Asian duopoly.

Secondly, Europe needs a reliable communication network operated and administered in the public interest. Individual interests should only be provided space where they align with the general interest. Precisely the opposite is the case in Europe today. The Internet consists of national networks, each with its own set of controllers, respectively pursuing particular interests. In theory, the Internet comprises the networks of various Internet service providers (ISPs), which are joined at neutral points (Internet exchange points) to create the network of networks. In practice, the notion of neutrality is questionable. DE-CIX is the largest of the worldwide 321 Internet exchange points and belongs to the Association of the German Internet Industry (eco). DE-CIX is run in a manner that grants access to the German intelligence service BND, thus compromising the data of primarily non-German entities. One may doubt whether this procedure safeguards European interests.

Thirdly, diverse new challenges arise with respect to cloud computing and distributed data processing and storage. The problem for positive regulation of European data and consumer protection is that the legal and economic spaces are not necessarily identical. Where data and access requests are outside the reach of European law enforcement, European legislation is toothless. The danger of major data theft from cloud platforms lurks above all when servers are located outside of Europe. Furthermore, terms of business that grant access rights to third parties can have unforeseen consequences. Not only do US providers have to hand over data stored on European

servers when requested (see the case of Microsoft Ireland versus the US Department of Justice) but European firms operating in the United States are also subject to the same obligation.

Fourthly, the digitalisation of communication has hollowed out the right to privacy. As the Snowden revelations demonstrate, state security agencies can access and analyse unencrypted e-mails whenever they wish. Yet privacy and liberty are fundamental conditions for the market itself and therefore require protection. In liberal societies the right to privacy is also constitutive, for without privacy there can be no liberty. The endangerment of data privacy and consequently social liberty calls for a European response. Because telecommunications and information infrastructure is in private ownership and networks transcend national borders, the emphasis is currently on improving encryption methods. However, encryption technologies must come without any hidden access options (back doors) demanded for investigation purposes not only by the Chinese government but also by its US and British counterparts. A great deal of information can also be gleaned from encrypted e-mails. The metadata – so to speak the envelope containing the message – reveals who is in contact with whom, when and how often, and even the subject line of the message.

Fifthly, quasi-monopolies of major corporations are fundamentally problematic. Cartels and other forms of market domination lead to higher prices, inferior products and grave deviations from the ideal of the free market. Although merger controls do exist, European competition law oftentimes does not respond with sanctions until market domination has actually led to abuses. Nonetheless, there is currently extensive discussion on whether US technology giant Google occupies a market-dominating position in Europe. In November 2010, then EU Competition Commissioner Joaquín Almunia opened a case against Google, which his successor Margrethe Vestager has now revived after collating extensive evidence that Google's search results systematically favour its own services over those of its rivals. The Competition Commissioner is also taking action against several states that may have granted corporations such as Amazon and Apple advantages through tax rulings. If individual companies hereby benefit at the cost of their rivals, this constitutes a violation of competition law.

Deepening Digital Integration

Historically, regulatory challenges of the kind illustrated using the virtual path of an email have often contributed to ambitious leaps in European integration. The most striking example is the creation of the internal market through the Single European Act in 1987. In order to deepen digital integration, Andrus Ansip, Vice President of the European Commission for the Digital Single Market, and Günther Oettinger, Commissioner for the Digital Economy and Society since November 2014, are therefore pushing hard for the establishment of a digital single market. The objective is to expand the advantages of the European internal market to the digital sphere. According to the Commission, we will only benefit from the technical innovations associated with big data, cloud computing and the Internet of Things, if attempts at digital sovereignty are overcome in favour of a European harmonisation of national markets. The April 2014 ruling of the European Court of Justice, overturning the Data Retention Directive and demanding greater data protection and security on the basis of European law, can be considered an instigator for initiatives to realise the digital single market. The ruling sets legal limits on the storage of information of EU citizens in third countries and provides economic incentives for establishing a European network infrastructure.

The Strategy for a Digital Single Market

The Digital Single Market Strategy published by the European Commission at the beginning of June 2015 comprises sixteen measures to be implemented by the end of 2016. It is based on three pillars: 1) better access to digital goods and services for consumers and businesses across Europe; 2) the creation of infrastructure for digital networks and services and 3) the exploitation of growth potentials of the digital economy.

By virtue of market-creating measures defined in the first pillar, companies in the digital single market should experience no (or only minimal) obstacles compared to national commerce (negative integration). To this end, contract law and VAT rules are to be harmonised and cross-border data delivery services improved. The strategy also has the goal of ending access restrictions (geo-blocking), for example by standardising copyright law. The Commission wishes to reduce barriers to e-commerce, harmonise tax rules, investigate the market power of online platforms such as search engines and social networks, and reform the legal framework for audio-visual media.

As part of the second pillar, the Commission proposes new rules (positive integration). The planned NIS Directive will make operators of critical infrastructure liable for failures. Apart from having to ensure better IT security, providers of services such as trading platforms, payment systems, social networks, search engines and data clouds will be obliged to report serious cyber-attacks and will have to implement appropriate safeguards in line with the planned EU rules. The rights of the end user, as the weakest link in the chain, will also be strengthened by compelling providers to report security violations and loss of integrity (data falsification). Technical norms are to be harmonised and trustworthy cloud services certified. The Commission will also review the indemnifications for providers affected by the Electronic Commerce Directive and harmonise procedures for removing illegal content from the Internet (terrorist propaganda, child pornography, copyright violations). An extensive reform of copyright law is currently under discussion in the European Parliament.

The third pillar is about both expanding the European digital economy and supporting the increasing use of digital technology in conventional industry. Medium-sized businesses and start-ups are to be supported through easier access to investment capital, and the legal regulation of portability, interoperability and standardisation is to be improved with regard to cloud computing and big data solutions. The main thrust of the EU regulation is to prevent confidential data getting into the wrong hands on account of inadequate security or a defective legal framework. Restrictive laws on data location and encryption methods are to be harmonised so that all European market participants are treated equally in all respects. It is important to remember that data routing between places outside the United States, for example communication between Estonia and Italy, may still pass through US servers. The feared consequences for data protection lend weight to calls for restricting routing to the Schengen area. However, this is problematic for economic reasons and since it risks decreasing technical reliability. The US Trade Representative (USTR) regards it as a violation of international trade agreements – even though similar arrangements also exist in the United States.

A more convincing proposal comes from the European Network and Information Security Agency (ENISA). It contains possibilities for end-to-end encryption for various applications (securing data when sending and receiving as well as in transit). Methods for disguising metadata are also considered, for example using virtual private networks or onion routing to encrypt an e-mail multiple times. The encryption layers are then placed like envelopes around the actual message, with each party involved permitted access only to the information it requires to forward the message.

Data Protection as Competitive Advantage

To counteract illegal exploitation of content and data on the Internet, copyright, data protection and consumer rights are also to be refined at the national and European levels. The aim of the planned European General Data Protection Regulation (GDPR) is to enforce data protection in order to improve legal certainty for businesses in the internal market. In June 2015, after more than three years of negotiations, the EU interior and justice ministers agreed on a joint position towards reform of data protection rules. The proposal is now under discussion in the Trilogue between European Council, Commission and European Parliament. The new GDPR is intended to come into force in 2018 to replace the Data Protection Directive of 1995. It proposes to compel businesses to implement strong default privacy settings in their technologies, enable class action suits over privacy violations, improve cooperation between national regulators, and create a harmonised oversight mechanism. Not least, sanctions in response to data protection violations are proposed. While the original draft of the European Commission sets these at two percent of the company's global turnover, the European Parliament calls for the fine to be set at five percent of annual turnover and at least €100 million.

The "right to be forgotten", which the Spaniard Mario Costeja González won from Google in the European Court of Justice ruling of 13 May 2014 and which has transformed Europe's digital economy, is a central point in the GDPR. The ruling states that search engines must observe valid data protection directives and cannot fall back on American law even if the parent company is headquartered in the United States and its data are processed there. Every EU citizen now has the right to demand for the search engines to delete their personal information. Google alone, according to its own figures, had received 293,004 deletion requests by 6 August 2015, 41.3 percent of which had been fulfilled.

Under Article 23 (1) of the GDPR, data protection must in the future be integrated directly into processes, systems and products. Sensitive data from EU citizens may only be passed to foreign security agencies under the terms of a judicial assistance agreement. Under current law, it is forbidden to transfer personal data from member states to countries that do not possess data protection comparable to European law. This is an important issue, because the European constitutional understanding diverges significantly from the American one. In the United States the focus is not on the protection of human dignity, but on freedom in the sense of *liberty* as a civil right of the individual, who wishes to be "free of legal regulations". But the new GDPR and the proposed directive on personal data protection in law enforcement are aimed at implementing legal guarantees for EU citizens in the judicial assistance system. The data protection reform package will therefore have repercussions on all new bilateral agreements with the United States on data transfer in the areas of security and economy. This includes among others the exchange of personal data, the data protection umbrella agreement, the bilateral mutual legal assistance agreement, and the exchange of airline passenger data.

Europe in the Digital World

The European regulatory system is not restricted to the internal market, but also has a global dimension. The European information and communications sector is closely interconnected with other markets. In order to take account of the reciprocal dependencies of European and global standards and rules, the European Commission and individual member states have become active in international bodies on the central issues of Internet Governance and cybersecurity. For this reason, digital integration also comprises a foreign policy dimension affecting not only the expansion of the

digital internal market beyond national borders but also the member states' cyber foreign and security policy. Accordingly, the European Council conclusions on Internet Governance of November 2014 and on cyberdiplomacy of February 2015 call for a "multi-stakeholder approach", including representatives of business, the technical community, science and civil society as well as governments. Furthermore, they demand close cyberdiplomacy with the United States, for example in the Group of Governmental Experts (GGE) at the UN level.

In the relevant documents on European cybersecurity of February 2013 and on Internet Governance of February 2014, the European Union argues that freedom, security and stability are vital for the safeguarding of cyberspace. Internet Governance refers to the development and application of shared principles, norms and approaches in global communication. Since June 2011, the European Commission has been pursuing the objective of creating "a single, open, free, unfragmented network of networks, subject to the same laws and norms that apply in other areas of our day-to-day lives" (in EU terminology: COMPACT). In order to prevent state influence from eroding the multi-stakeholder approach, the European Union intends to strengthen the role of the Internet Governance Forum (IGF), the global multi-stakeholder forum with 3,700 members from 144 countries (2014). The UN General Assembly will decide at the end of 2015 whether to continue the format. At the same time, the European Union is calling on the organisations managing the Internet to "internationalise". This primarily concerns ICANN (Internet Corporation for Assigned Names and Numbers), which is responsible for the stable functioning of the Internet, and its IANA department (Internet Assigned Numbers Authority), which assigns numbers and names on the Internet, above all IP addresses. The European Union wishes to prevent individual states or private interests from dominating the administration of Internet resources. Therein, the EU is (at least officially) at loggerheads with the United States, which plays a leading role in ICANN. The process of preparing improved accountability procedures, for example to challenge decisions of the ICANN Board, is ongoing. ICANN CEO Fadi Chehadé has already stated that it will not be possible to complete the hand-over of oversight of core Internet administrative functions by September 2015 as planned. Therefore, he said, ICANN will be extending its contracts with the US Department of Commerce.

Another arena of multi-stakeholder discussion was the NETmundial conference in 2014, where the focus was on human rights and the right to privacy on the Internet. As a result, a European, the Maltese Joseph Cannataci, was appointed as the first UN Special Rapporteur on the Right to Privacy by the UN's Human Rights Council in July 2015.

Moreover, at the initiative of the World Economic Forum (WEF), the Brazilian Internet Steering Committee (CGI) and ICANN, the so-called NETmundial Initiative (NMI) was launched in January 2015. However, with European participants criticising its composition and lack of distance to the IGF, it has yet to establish a place for itself in the Internet governance ecosystem.

In an open letter of April 2015, Federica Mogherini, High Representative of the European Union for Foreign Affairs and Security Policy, and Dutch Foreign Minister Bert Koenders lay out the European Union's lowest common denominators. They point out the necessity to hold states responsible for attacks originating from their own national cyberspace and emphasise that inadequate protection of central infrastructure represents a threat not only to national but also international security.

This lowest common denominator was promoted by five EU member states in the fourth round of the UN Group of Governmental Experts (GGE) on cybersecurity (altogether representing twenty governments: Antigua and Barbuda, Belarus, Brazil [chair], China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya,

Malaysia, Mexico, Pakistan, Russia, Spain, United Kingdom, USA). Diplomats in the GGE analyse security risks in cyberspace and develop confidence building measures (CBM) as well as starting points for cooperation. The last session of the fourth round was held in New York in late June 2015; its final report has yet to be adopted by the UN General Assembly. The concrete application of international law to cyberspace continues to be a source of conflict. Incompatible interpretations of information security make a substantive discussion at the UN level almost impossible. Contested issues include the scope of issues to be discussed, differing threat perceptions, and the envisioned role of the UN and governments vis-à-vis private-sector and civil society actors. While there is broad agreement that states must be held responsible for their behaviour in cyberspace, Germany and the United States regard current international (humanitarian) law as the sufficient legal starting point for cyberspace, while Russia, China and other states demand the development of specific international law for cyberspace. The G-77 states are above all interested in discussing the topic of cybersecurity in an open working group or carrying it into the Geneva Conference on Disarmament. The European Union does not operate as a monolithic bloc at the UN level, but coordination exists between Germany, France and the United Kingdom. This coordination also includes other like-minded Western countries in the group. With Russia already calling for a fifth round of GGE discussions, we have reason to believe that the EU member states represented there will have to keep a stronger eye than ever on European interests.

Requirements for German Politics

Many regard the EU's overall digital strategy as without ambitions and incapable of advancing Europe's digital assertiveness vis-à-vis the United States and China. Even large member states like Germany can exert global influence only in cooperation with EU institutions and other member states. The Friends of the Presidency Group on Cyber Issues (FoP Cyber) coordinates within Europe to support the respective EU Council Presidency, and should also expand its remit to international organisations. The EU's digital assertiveness requires additional international flanking measures in order to stabilise the values of freedom and democracy in Europe and generate greater global traction. As part of the 2014 Digital Agenda, the German government has stated its intent to take "measures to regain technological sovereignty" and to create "a European area of trust". In the logic of negative and positive integration (Scharpf), technological sovereignty in the internal market would be legitimate only where it does not undermine significant achievements of social market economy and democracy. The internal market is based on fundamental trust in the forces of the free market and principles of openness and non-discrimination. Scepticism is therefore warranted towards the establishment of heavily subsidised national or European companies. State intervention is only appropriate where the market fails in providing important goods such as data security and privacy. Reciprocal global dependencies are not per se problematic, but become unacceptable when they undermine Europeans' ability to autonomously control their data and systems vis-à-vis illiberal governments. States that reject values such as the free market, democracy and human freedom should be regarded as second-choice sources of strategically important resources for European communication infrastructure. Purchasing rare earths from Australia, for example, is more expensive, but avoids political double standards.

The case of Estonia offers an example of a successful digitalisation strategy. With only about 1.3 million inhabitants, the country is a pioneer of digitalisation in Europe. Its national e-ID infrastructure is used by more than 90 percent of its citizens. The digital ID card has a range of functions and can be used on the Internet wherever iden-

tity verification is required, for example for bank transactions or voting. Estonia operates largely without using Russian infrastructure and technology and has established a strong security network with eight international mirror servers in friendly states, including the United Kingdom, Germany, the United States, Canada, South Africa and Japan. As far as electronic governance is concerned, small countries like Estonia are considerably further advanced than the big EU member states.

The further the European Union advances its digital integration in the form of European law, the more it will strengthen its digital assertiveness, both within Europe and internationally. The market location principle, a central instrument of the internal market, guarantees equal treatment of domestic and foreign businesses. Digital assertiveness depends crucially on the willingness of member states to expand the quantity and quality of European law. Only the European Union has the potential to forge a third way outside of the technological dominance of the United States and China, not individual member states.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1861-1761

Translation by Meredith Dale

(English version of SWP-Aktuell 71/2015)