SUMMARY
The current global debates about the role of governments in internet governance and the application of international law in cyberspace will have significant impact on the future of the internet. With a view to shaping their outcome, the EU is focusing on a number of priority areas: protecting the digital economy, reducing cybercrime, enhancing international stability, protecting the free and open internet, and capacity-building in third countries.

The need for closer engagement with key international partners, as a way towards promoting the EU's political, economic and strategic interests was recognised in the EU Cybersecurity Strategy of 2013, and the Council Conclusions on Cyber Diplomacy adopted in February 2015. The EU is pursuing this objective through cyber dialogues with China, India, Japan, South Korea and the United States, as well as other consultation venues where cyber issues are among the agenda items.

With internet and new communications technologies becoming an integral component of everyday life, the European Parliament plays a crucial role in ensuring that internet and digital technologies strengthen, rather than undermine, human development. It can do so through legislation and agenda-setting, parliamentary diplomacy and capacity building, awareness raising and its budgetary powers.

In this briefing:
- Cyber diplomacy: what is at stake?
- EU's engagement with third countries
  - China
  - India
  - Japan
  - South Korea
  - United States
- Mainstreaming cyber issues in the EP
- Main references
Cyber diplomacy: what is at stake?
The EU Cybersecurity Strategy presented in February 2013 lists stronger relations with international partners as one of the mechanisms towards preserving open, free and secure cyberspace. In February 2015, the Council of the EU adopted Council Conclusions on Cyber Diplomacy which recognise engagement with key partners as a way towards promoting EU political, economic and strategic interests.¹ The document also elaborates on five main areas of the EU’s cyber diplomacy: promotion and protection of human rights in cyberspace, norms of behaviour and application of existing international law in the field of international security, internet governance, enhancing competitiveness and prosperity, as well as capacity-building and development. A number of cross-cutting and interlinked priorities can be traced in all of these policy areas.

Priority 1: Protecting the digital economy
Recognising the internet’s impact on growth, jobs and prosperity, the protection of cyberspace against cyber espionage and attacks on critical infrastructure has become a key component of national security and cybersecurity strategies. With the number of internet users expected to reach 4.7 billion by 2025, the number of mobile devices already higher than the world’s population, and rapid technological advances, promotion of the EU’s regulatory framework and standards in cyberspace is an important part of economic diplomacy. The EU already plays an important role in the field of privacy and data protection, in particular concerning the regulation of cross-border data flows. The European Commission proposal for a directive concerning measures to ensure a high common level of network and information security across the Union (commonly referred to as the 'network and information security' directive) was presented in 2013. If eventually adopted, this text could become a global cybersecurity benchmark and further strengthen the EU’s global standing. However, the legally binding nature of the obligations that this legislation might impose is not fully compatible with the voluntary mechanism opted for by others, notably the US.

Priority 2: Reducing cybercrime
As the digital economy becomes an important component of industrial and service architectures, it also attracts the attention of organised crime groups or individual hackers as a relatively inexpensive way to make profits. The development of the 'malware as a service' (Maas) business has also made it easy for anyone to join the ranks of cybercriminals. The total cost of cybercrime is currently estimated at between US$375 billion and US$575 billion. This dynamic has pushed law enforcement agencies worldwide towards closer cooperation, and to improve the capacities of their international partners through regional or global initiatives. At the same time, diplomatic services are taking steps to de-escalate potential misunderstandings concerning breaches of critical national infrastructure. In addition, in order to ensure that the rights of victims and offenders are respected, the EU emphasises the importance of effective investigation and prosecution techniques that allow timely access to electronic evidence while fully respecting international law and fundamental rights. Many of these objectives are implemented through existing international instruments such as the Council of Europe Convention on Cybercrime or are enshrined – to a varied degree – in other regional initiatives.

Priority 3: Enhancing international stability
One of the main aims of the EU's cyber diplomacy is building global consensus on how to apply existing international law in cyberspace and develop norms for responsible
state behaviour. This objective is particularly relevant given that more than 30 states have already developed national cyber-military strategies, some of which go beyond purely defensive purposes and consider the cyber domain as a space for intelligence-gathering (UK Cyber Security Strategy) or provide for preventive cyber-attacks in defence of vital national interests (US Department of Defense Cyber Strategy). Since many issues related to the use of force in cyberspace still raise controversy, the EU supports international discussions on the norms of responsible state behaviour and application of international law in cyberspace. In that context, the EU follows closely the works of the UN Group of Governmental Experts on developments in the field of Information and Telecommunications in the context of international security. Some regional organisations have also accelerated their work on confidence-building measures (CBMs). The EU played an important coordination role in the adoption of the first set of cyber CBMs in the OSCE, and encourages similar efforts undertaken in other regional fora such as the ASEAN Regional Forum. The EU is also monitoring with concern the proposal for a Code of Conduct for Information Security made by the Shanghai Cooperation Organisation (SCO), which contains provisions that might have an adverse impact on respect for human rights and increase governments' control over the internet.

**Priority 4: Protecting the free and open internet**

One of the foundations of the EU's global engagement is the protection of human rights online. Consequently, the Council of the EU has adopted EU Guidelines on Freedom of Expression online and offline and EU Guidelines on Human Rights Defenders. According to these, the EU should protect and promote freedom of opinion and expression in its external action, including by preventing potential violations of these rights and reacting to concrete cases of violation. Issues like more universal access to the internet in developing countries, and curbing the uncontrolled export of technologies that could be used for surveillance or censorship by authoritarian regimes are also mentioned. At the same time, preserving an open and free internet is closely linked to the promotion and strengthening of the multistakeholder model of internet governance, extending the mandate of the Internet Governance Forum beyond 2015, the transfer of the stewardship of the Internet Assigned Numbers Authority (IANA), and strengthening the accountability of the Internet Corporation for Assigned Names and Numbers (ICANN).

**Priority 5: Improving capacities worldwide**

Acknowledging the benefits and risks associated with the spread of internet use around the world – including in developing countries – the EU has turned cyber capacity-building into a strategic building block of its diplomacy. The EU's primary focus is on ensuring that people around the world can fully develop their societal, political and economic ambitions through the use of free, open and secure internet. It does so by combining the EU development and security agenda in promoting the rule of law, strengthening instruments targeting cybercrime, increasing resilience of critical information infrastructure, and by reinforcing close cooperation and coordination among international stakeholders. Under the Instrument contributing to Stability and Peace, the European Commission has earmarked between €29.5 and €49 million for cyber capacity-building in its 2014-20 Thematic Strategy Paper, in particular for fighting cybercrime and improving the cybersecurity of critical infrastructure.

**EU's engagement with third countries**

In order to counter the risks of cyber-attacks and to achieve the priorities listed above, the EU launched cyber dialogues with China, India, Japan, South Korea, and the United
States. The European External Action Service (EEAS) is the coordinating body for these processes. In addition, sectoral dialogues are organised regularly by European Commission Directorates-General: on ICT (DG Communications Networks, Content and Technology), on law enforcement cooperation (DG Migration and Home Affairs), and on capacity-building projects (DG International Cooperation and Development, DG Neighbourhood and Enlargement Negotiations). Specialised agencies such as the European Union Agency for Network and Information Security (ENISA) and the European Police Office (Europol) have also increased their cooperation with third countries. Depending on the level of advancement in bilateral relations, the aims of these engagements range from information exchange and coordination of national policies to concrete initiatives at regional and global levels.

China
Recognising the importance of improving understanding and trust on cyber issues, the EU and China set up the EU-China Cyber Taskforce at the bilateral summit in Beijing in February 2012. The most recent meeting of the Task Force took place in November 2014 and reaffirmed their diverging views, in particular on governments’ role in cyberspace and the applicability of existing international law in cyberspace.

Policies and actors
China's internet population is among the fastest growing, and companies like Alibaba, Baidu and Tencent are among the biggest internet companies in the world. This growth has been matched by more decisive political actions at both domestic and international level. China’s activity on the international stage is also a reaction to accusations about cyber-attacks originating from its territory and targeting foreign governments and companies. China's cybersecurity legal framework comprises criminal law, a number of decisions, administrative regulations and self-regulatory approaches promoted by the Internet Society of China. Specific regulations prohibit illegal hacking in companies' systems and the dissemination of information damaging state security. China declares its support for a ‘multilateral, democratic and transparent internet governance system’ that ensures ‘equal participation, balanced distribution of cyber resources and joint management of key infrastructures’. However, the instrumental and selective use of such statements to advance China’s political objectives raises questions about its real commitment and intentions. Even though China states its commitment to a multistakeholder model of internet governance, it also emphasises the government’s leading role in shaping the regulatory environment. In 2014 China organised the World Internet Conference in Wuzhen with the aim of building two main platforms: on connectivity between China and the world to stimulate the discussion about development, security and the use of the internet; and on common governance and the use of the internet in China.

Issues in EU-China relations
In principle, the EU and China agree that a secure and reliable internet is a key element in fostering economic growth. However, the EU remains cautious of ad hoc regulatory requirements discussed in China that may constitute barriers to trade, and as such would not only raise costs but also hinder innovation. For instance, the draft bank cybersecurity rules proposed in 2014 use national security as the basis for forcing technology vendors to hand over secret source code and adopt Chinese encryption algorithms. China, on the other hand, considers its approach justified as it is increasingly a victim of cyber-attacks and cyber-espionage from other countries. In China’s view, the planned cyber security review system does not constitute discrimination against foreign
businesses but rather is a solution modelled on other countries that, on security grounds, exclude Chinese companies from access to their markets. Many governments have denounced decisions taken by the Chinese government as a ‘tremendous barrier’ for foreign companies competing in the information technology sector. In March 2015, the National People’s Congress put on hold a controversial draft counterterrorism law which requires companies to keep servers and user data within China, to supply law enforcement authorities with communications records, and to censor terrorism-related internet content.

China’s interference with privacy and human rights – including through censorship tools like Great Firewall and Great Cannon – is one of the main constraints on closer cooperation. Proposals for cybercrime information-sharing, and cooperation in cybercrime cases originating from China are not being pursued for the moment due to the EU’s concerns about their potential negative impact on human rights. Contrary to the EU’s position, which favours law enforcement cooperation on the basis of the Budapest Convention, China supports the creation of a new UN legal instrument on cybercrime. For the moment, China is pursuing its objectives in the fight against cybercrime in alternative regional fora like the Regional Counter-Terrorism Structure of the Shanghai Cooperation Organisation (RCTS), ASEAN Regional Forum (ARF) and Asia-Pacific Economic Cooperation (APEC).

China is also engaged in shaping the narrative about states’ behaviour in cyberspace. Even though the EU and China are continuing discussions concerning the application of international law in cyberspace, there is still no consensus on some crucial aspects. China is particularly keen on maintaining control over its cyberspace, which translates into unequivocal support for the principles enshrined in the UN Charter, such as state sovereignty, non-interference and non-use of force. Even though a common position on cyber norms is still to be adopted by the Council, its Conclusions on Cyber Diplomacy affirm the EU’s commitment not only to the UN Charter but also to international humanitarian law. While the EU supports the existing processes on norms of behaviour – like the United Nations Governmental Group of Experts (UN GGE) in which several EU Member States participate – it remains cautious of other initiatives, like the Code of Conduct for Information Security proposed by the SCO. Additional insights to China’s view on cyber norms can be drawn from the cyber non-aggression agreement signed by China and Russia on 8 May 2015.

India

The political basis for the EU Cyber Dialogue with India was provided at the EU-India summit in 2010. The first meeting was held at the EU Joint Research Centre in Ispra in November 2011 and was followed by a meeting in New Delhi in 2012. After a three-year break, the issue was placed on the agenda of the EU-India Summit in 2015. The most recent round of the EU-India Cyber Dialogue took place on 21 May 2015.

Policies and actors

Like China, India is experiencing rapid growth in the percentage of its population online. That implies that, as more citizens are connected to internet, cybercrime is no longer a purely urban phenomenon. The 2013 data released by the Indian National Crime Records Bureau show that hacking accounted for almost 60% of all cyber-offences in 2013 and more than half of it originated in small towns or rural areas. Cyber threats range from less sophisticated fraudulent herbal medicine trade schemes, banking frauds based on stolen credit card information to more advanced cyber-attacks. India – like
other countries in south-east Asia – has been targeted by cyber-espionage operations against government and commercial networks. As one of the main technology and service hubs, India treats cybersecurity as a means to strengthen and protect its innovative potential. In January 2015, the government of Talangana – a southern Indian state – announced the plans to attract further investment to the region and to develop the T-Hub expected to be India’s biggest incubation facility. It is also expected that the 'Internet of Everything' as the foundation of citizen services, including infrastructure, utilities and governance on demand, will play a key role in the transition to Digital India. India is also at the forefront of employing ICT for development. Indian farmers have benefited from the e-Choupal project, which rapidly became the largest internet-based intervention initiative in rural India.

In 2013, the government adopted the National Cyber Security Policy which places particular focus on the development of indigenous security technologies and public-private cooperation. As part of the effort to fight cybercrime, the Indian government strengthened the law-enforcement component and expanded the state’s control over the internet, often at the expense of civil liberties. In its landmark ruling on the Information Technology Act, the Supreme Court of India struck down section 66-A which ‘arbitrarily, excessively and disproportionately invades the right of free speech’. In addition to setting up local computer emergency response teams (CERTs) to deal with imminent threats, the central government has created cyber operation centres to protect confidential information in the defence sector. Furthermore, India’s network of bilateral relationships is expanding. India has also sought Japan’s assistance on the latest technologies and expertise to tackle internet espionage, cyberterrorism and theft of personal as well as critical data. CERT-In and Japan-CERT have signed a Memorandum of Understanding for the exchange of information on the latest threats and vulnerabilities and mitigation strategies for cyber-attacks. In addition, as a consequence of a cyber-attack on the Eastern Command headquarters in Vishakapatnam, India is contemplating setting up a dedicated cyber command that would ensure doctrinal unity, streamline resources and coordinate defensive and offensive capabilities. India intends to train half a million cybersecurity professionals by 2018.

Issues in EU-India relations
Despite agreement on several issues, EU-India cooperation is weakened by India’s stance on the Budapest Convention. Despite the fact that the principles of the Convention served as inspiration for amendments to Indian legislation, the government remains critical of the Convention as a text not sufficiently reflecting the positions of developing countries. The fact that India has not thrown its weight behind alternative approaches pushed forward by China, and remains a ‘swing state’ in the debate leaves some room for optimism. The same is valid for India’s view on the future of internet governance. Even though India recognises the validity of the multistakeholder model, it still wishes to preserve the primary role of governments in what some analysts describe as 'smart multilateralism'. This stance was reaffirmed by India’s refusal to sign the final statement at the NETmundial conference hosted by Brazil's government in April 2014.

Japan
The EU-Japan Cyber Dialogue was established at the 22nd EU-Japan Summit in May 2014 in order to promote cooperation on cyberspace, through exchanges of their respective experience and knowledge. The first round of the Dialogue took place in Tokyo on 6 October 2014.
Policies and actors

In November 2014, Japan adopted the Cybersecurity Basic Act that addresses the definition and principles of cybersecurity. It established the Cybersecurity Strategy Headquarters (CSH), which is an enhanced version of the Information Security Policy Council responsible for the adoption of Japan’s Cybersecurity Strategy in 2013. Its main function is promoting cross-sectoral information security policy across the public and private sectors. The work of CSH is supported by the National Centre for Incident Readiness and Strategy for Cybersecurity. The Act obliges all relevant ministries to provide information about attacks. To handle cyber-attacks against military targets, the Ministry of Defence launched the Cyber Defence Unit with about 90 staff members. The Command, Control, Communication, and Computers Systems Command (C4SC) of Japan's Self-Defence Forces provides guidance and supervision for the CDU. It also ensures adequate maintenance and operation of the Defence Information Infrastructure (DII) System and Central Command System. Just in 2014, the MoD
allocated US$200 million for cyber-related activities, including for the development of the DII and information-gathering and analysis devices for cyber-defence.

**Issues in EU-Japan relations**

The EU and Japan share a vision of a free, secure and open internet. Both sides agree on the importance of multistakeholder processes and that existing international law applies in cyberspace. Japan was the first Asian country to ratify the Budapest Convention. The EU and Japan face similar challenges concerning the fight against cybercrime, countering cyber-espionage, and securing the business environment. In terms of international cooperation, Japanese priorities include building global response mechanisms and partnerships (e.g. information sharing, response to cyber-crime), raising cybersecurity standards, and developing international rule-making for cybersecurity (international standards). Japan is committed to the promotion of existing international law in cyberspace, including the UN Charter and international humanitarian law, but – like the EU – agrees that further reflection is needed on how these acts should apply in cyberspace, especially with regard to territorial sovereignty and state responsibility. To that effect, Japan is involved in the ASEAN debates about CBMs for cyberspace (which the EU also supports), information security, transnational crime, and capacity-building. Japan also promotes joint cooperation in the Japan-ASEAN Security Partnership (JASPER) and Internet Traffic Monitoring Data Sharing Project (TSUBAME Project).

**South Korea**

EU cyber-policy consultations with South Korea (Republic of Korea) were formally established at the EU-South Korea Summit in November 2013 as a component of the future-oriented partnership aimed at strengthening cooperation and collaboration on bilateral, regional and global issues. The exploratory cyber consultation took place in May 2014 and resulted in the decision to launch a formal Cyber Dialogue. The first EU-South Korea Cyber Dialogue took place on 29 April 2015 in Seoul.

**Policies and actors**

South Korea's approach to cyberspace is shaped by two factors. As one of the most internet-connected nations in the world, South Korea pursues the 'creative economy' model – a process of creating new jobs and industries through converging science, technology, industry and ICTs. At the same time, South Korea has to deal with the permanent threat posed by North Korea. The latter is suspected to have orchestrated several cyber-attacks on South Korean computer systems, including the March 2013 attack on television stations and banks, and December 2014 cyber-attacks on Korea Hydro and Nuclear Power. In this specific context, the Korean National Cyber Security Master Plan was adopted in 2011. The National Cyber Security Centre was established as the main point for identifying, preventing and responding to cyber-attacks. In 2013, the Ministry of Science announced its intention to train 5 000 cybersecurity experts by 2017. In addition to improving its own capabilities, South Korea pursues its policy objectives through a broad network of international initiatives. The capacity-building expertise of the Korea Internet and Security Agency (KISA) is one of the most sought-after. In 2013, the Seoul Conference on Cyberspace resulted in the adoption of the Seoul Framework for and Commitment to Open and Secure Cyberspace, which offered guidelines on coping with cybercrime and reaffirmed the importance of internet access for human development. In March 2015, South Korea hosted a workshop organised by the Cyber Secretariat of the Forum for East Asia-Latin America Cooperation – the only
multilateral intergovernmental consultative mechanism between East Asia and Latin America, which brings together 36 countries.

**Issues in EU-South Korea relations**

South Korea is the only country with which the EU has concluded framework agreements on political affairs, the economy, and global security. The range of cyberspace issues on the EU-South Korea agenda includes the exchange of best practices in fighting cybercrime and enhancing cybersecurity, promotion of human rights online, and consultation on a number of issues, including international security, capacity-building and R&D. With regard to international security, both sides agree that international law applies in cyberspace, and is crucial to maintaining a secure, open and stable internet. South Korea and the EU also share the view that the internet is an enabler for sustainable development and can be a particularly relevant element in expediting the integration of developing countries into the global economy. The latest round of the Cyber Dialogue also focused on exchanges of information concerning the hacking incidents involving Korean nuclear facilities and Sony Pictures Entertainment.

**United States of America**

These issues on the transatlantic agenda are primarily pursued through the EU-US Cyber Dialogue, established in the aftermath of the EU-US Summit on 26 March 2014. The EU-US Cyber Dialogue takes forward the expert-level cooperation within the EU-US Cybersecurity and Cybercrime Working Group established in 2011, by adding an international and strategic dimension to transatlantic cyber relations. Cooperation in the EU-US Working Group on Cybercrime – in particular to support the Global Alliance to fight child sexual abuse online – is very successful. Another venue – the EU-US Working Group on Cybersecurity – works along several strands, focusing on public-private partnerships and incident management. Many good examples of cooperation exist at the operational level. In April 2015, a multinational law enforcement operation led by the European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT) disrupted the operations of the Beebone botnet, that had installed malware on about 12 000 computers in around 195 countries.

**Policies and actors**

The US approach to cyber-threats – as laid out in the Strategy for Cyberspace of 2011 and numerous additional acts – is a mixture of law enforcement, development, diplomatic and military measures. Consequently, most of the government’s efforts focus on improving coordination between the main actors (i.e. Department of Homeland Security, Department of State, and Department of Justice). For instance, in February 2015, the Department of Homeland Security established the National Cybersecurity and Communications Integration Center – a 24/7 cyber situational-awareness, incident response, and management centre that integrates data from the federal government, the intelligence community, and law enforcement agencies. Such a comprehensive approach allows the government to come up with new ways of addressing cyber-threats. In April 2015, President Barack Obama signed an Executive Order authorising the Treasury Department to use economic sanctions against hackers or companies deemed to be engaged in cyber-attacks threatening the national security, foreign policy, economic health or financial stability of the US. This decision follows sanctions introduced by the US against North Korea in January 2015. The FBI has started adapting traditional investigative techniques to cybercrimes, as evidenced by the indictment of a former employee of the Department of Energy and the Nuclear Regulatory Commission for an attempted cyber-attack and the intention to sell US nuclear weapons secrets to a...
foreign government. In addition, the Cybersecurity Forum for Independent and Executive Branch Agencies, an inter-agency group spearheaded by the Nuclear Regulatory Commission, was launched to explore different approaches to cybersecurity, including through voluntary mechanisms rather than regulation.

With regard to international security, the key objective of EU-US dialogue is to seek greater stability in cyberspace and support ongoing efforts in this respect, including in the United Nations Governmental Group of Experts (UN GGE) and regional fora such as the OSCE, ARF and Organization of American States. Both the EU and the US promote the view – agreed by the UN GGE in 2013 – that existing international law is applicable to cyberspace. At the same time, EU Member States and the US work closely together in international fora with the aim of elaborating a set of CBMs and norms of state behaviour in cyberspace. With regard to the latter, the peacetime norms proposed by the United States to preserve stability in cyberspace include: abstaining from cyber-attacks that could damage or impair critical national infrastructure; refraining from disrupting the work of CERTs and CSIRTs; and cooperating with other nations’ law enforcement agencies in investigating cybercrimes. In April 2015, the US Department of Defense presented the new Defense Cyber Strategy (DCS) that addresses the Pentagon’s three main cyber missions, including 'defending the United States and its interests against cyber-attacks of significant consequence'. DCS also laid the foundations for a 'preventive cyber-offence doctrine', whereby the President may authorise the US military to conduct cyber-attacks to counter an imminent or ongoing attack. The Pentagon is also continuing efforts to build a Cyber Mission Force (CMF) that will eventually include nearly 6,200 military, civilian and contractor-support personnel.

The United States has established a number of bilateral cyber dialogues with other countries but most of them are currently on hold, Japan and South Korea being notable exceptions. The US-India Cyber Dialogue has been on hold for two years. India's position on internet governance and the multistakeholder model, in particular, cause concerns among US policy-makers. Dialogue with China is much more complex and has been placed on hold following the indictment of five men in the People’s Liberation Army on cyber-espionage charges. In May 2015, Secretary of State, John Kerry visited China to lay the groundwork for the bilateral Strategic and Economic Dialogue in June 2015, however conflicting points on cybersecurity remain unresolved. The visit coincided with an FBI warning of a Chinese-based cyber-espionage campaign against US government network and businesses.

**Issues in EU-US relations**

Even though positions across the Atlantic are aligned on most of the issues (i.e. cyber norms, CBMs, internet governance, and capacity-building), a number of issues still require additional contacts between Brussels and Washington. This is particularly the case for law enforcement cooperation and investigative techniques. For instance, several civil society groups, businesses and cybersecurity experts have criticised an internal review of encryption policy options – including built-in exceptions to encryption for law enforcement – being prepared for President Obama. The criticism from the private sector is particularly problematic given the importance of private-public partnerships for enhancing cybersecurity. It makes clear that, even though IT companies and industry are willing to work with the government (e.g. to disrupt botnets), they are not willing to take steps that could undermine their clients' trust.
Another issue on the transatlantic agenda that requires close coordination is the future of internet governance. In the November 2014 Council Conclusions on Internet Governance, the EU welcomed the intention by the US National Telecommunications and Information Administration to transfer key internet domain-name functions by 30 September 2015. The United States admits that the transfer of the IANA function to another organisation before that deadline would be the best-case scenario but there is a possibility that an extension of the deadline will be necessary in order not to jeopardise the stability and robustness of internet infrastructure or the multistakeholder model.

Mainstreaming cyber issues in the European Parliament

Even though the European Parliament (EP) is not formally involved in any of the cyber dialogues established between the EEAS or the European Commission and third countries, it has numerous ways of influencing the process, including through legislation and agenda-setting, parliamentary diplomacy and capacity-building, awareness-raising, and budgetary means.

- **Legislation and agenda-setting:** As a co-legislator, the European Parliament exercises significant influence over the shape of EU law in a number of relevant policy areas, including networks and information security, protection of critical infrastructure, the fight against cybercrime, protection of privacy and personal information, standard-setting, and international agreements. Some of the acts adopted may also have an impact beyond EU territory (e.g. data protection) and become a global standard. In addition, under Article 225 TFEU, the EP may request the Commission to submit any appropriate legislative proposal. Specialised committees (e.g. AFET, SEDE, DROI, INTA, DEVE, LIBE and ITRE) through reports and opinions play a crucial role in shaping the EP’s positions in their respective areas of expertise. The European Parliament also enjoys a range of supervisory powers which can be used to influence EU policies. The European Parliament, for instance, has the right to be informed and consulted on CFSP/CSDP aspects. Article 36 TEU compels the High Representative to regularly inform and consult the EP on foreign policy.

### Examples of cyber-relevant resolutions adopted by the European Parliament

**Geographic:** Resolution on a broader Transatlantic Partnership, Resolution on EU-China Relations, Resolution on the Future of EU-ASEAN Relations,

**Thematic:** Fight against child sexual abuse on the Internet, Renewal of the mandate of the Internet Governance Forum, Digital Single Market, Resolution on the Implementation of CSDP

- **Parliamentary diplomacy and capacity-building:** Through its committees, delegations and other bodies, the EP maintains an extensive network of working relations with third countries, including with those who have not yet established cyber dialogues with the EU. Depending on the scope of a bilateral relationship, the European Parliament may decide to establish interparliamentary delegations, delegations to parliamentary assemblies or joint parliamentary assemblies (see map 1). These venues provide an opportunity for discussing issues of common concern, shaping the partner countries’ positions and indirectly strengthening their domestic legislative processes. For instance, the Transatlantic Legislators’ Dialogue – a unique venue for cooperation between the EP and the US Congress – has dealt with cyber issues in the past. Furthermore, study visits organised by the European Parliament for parliamentary delegations from third countries contribute to building and improving their law-making capacities.
• **Awareness-raising**: Transparency and openness of the European Parliament’s deliberations (i.e. access to documents, web streaming of plenary sessions and committee meetings) offer a unique possibility for raising awareness of cyber-related issues. Public hearings, expert workshops, events and direct interactions of MEPs with their constituencies and other stakeholders may be used to explain specific policy positions to a broader audience and raise their awareness of cyber-threats and also the opportunities stemming from the digital environment.

• **Power of the purse**: By virtue of the EU Treaties, the European Parliament shares budgetary powers with the Council and votes on the entire EU budget. This includes, among other things, decisions on the annual CFSP budget, the EU’s external financial instruments (i.e. Instrument contributing to Stability and Peace, European Neighbourhood Instrument) and the mandates and budgets of other relevant EU agencies and bodies like ENISA or the European Cybercrime Centre within Europol.

If the European Parliament mainstreams cyber-related issues into all areas of its activity and uses the instruments at its disposal, it will reinforce its role in ensuring that internet and ICTs contribute to bolstering human development.

**Endnotes**

1 Cyber diplomacy as a policy area focused on economic, security and political aspects of cyberspace is different from digital diplomacy which considers ICTs as one of the tools in diplomacy.


3 On behalf of the United States Government, through a contract with NTIA, ICANN performs the IANA functions, including managing the internet Domain Name System.

4 The EU has also established close cooperation with a number of international and regional institutions, including the UN, NATO, Council of Europe, OSCE, ASEAN, and Organisation of American States. In addition to Track I political processes, the EU and its Member States continue the discussions about cyber-related issues through Track II initiatives, like Sino-European Cyber Dialogue with China or the involvement in the Northeast Asia Peace and Cooperation Initiative (NAPCI) with South Korea.

5 The Great Cannon is similar in many ways to the use of QUANTUM by the US National Security Agency.

6 Many cyber defence issues on the transatlantic agenda are also pursued through informal staff-to-staff cyber consultations between EU and NATO. In November 2014, the Council of the EU adopted the Cyber Defence Policy Framework that aims to reinforce the resilience of Common Security and Defence Policy missions, operations and structures.

**Disclaimer and Copyright**

The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. It is addressed to the Members and staff of the EP for their parliamentary work. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2015.

Photo credits: © alphaspirit / Fotolia.

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://epthinktank.eu (blog)