UACES 46th Annual Conference

London, 5-7 September 2016

www.uaces.org

Paper submitted to UACES 2016 annual conference, London, September 2016.
DRAFT PAPER – DO NOT QUOTE OR CITE

EU cyber diplomacy: The purposes and mechanisms of EU cyber partnerships with third countries

THOMAS RENARD[1]

ABSTRACT: The European Union is increasingly active on cyber issues internationally, guided by its various foreign policy documents and strategies, including its 2013 Cybersecurity Strategy and the 2015 Council conclusions on cyber-diplomacy. In line with these documents, the EU has deepened its bilateral ties with a number of key countries, resulting in a network of cyber partnerships. This article explores these partnerships in depth. It seeks to explain the different types of purposes that they fulfil, and the various mechanisms that underpin them, based on an ambitious mapping exercise. In essence, it is argued that the EU's cyber partnerships aim not only for bilateral cooperation, but also for 'reflexive' results (whereby the EU aim to develop its cyber and diplomatic agency) and 'structural' results (whereby bilateral partnerships aim to strengthen the multilateral fabric and global internet governance). Once assessed against these multiple and intertwined purposes, these cyber partnerships appear more useful than meets the eye.

KEY WORDS: European Union (EU); cyber; diplomacy; strategic partnerships; CFSP; internet

1. Introduction

Cyberspace is an area of regular tensions and conflicts among global powers. The United States (US) has accused China, Russia, Iran and North Korea of carrying cyber attacks against its public administration and its private sector,[2] whereas the US has used itself cyber instruments to develop a massive spying programme, revealed by the former consultant Edward Snowden, and to attack other states, as illustrated by the Stuxnet programme.[3]

Diplomatic talks and international agreements have become essential to manage these tensions. In September 2015, the US and China concluded an important agreement facilitating cooperation on cyber-crime issues and aiming to curb cyber-enabled economic espionage. The agreement, which involves some mechanisms to ensure its implementation, followed a long diplomatic process that included a four-day high-level gathering earlier that month (Nakashima and Mufson, 2015). A few months earlier, Russian President Vladimir Putin and Chinese President Xi Jinping had inked a bilateral 'non-aggression' agreement for cyberspace, according to which they committed to avoid hacking and carrying out cyber-attacks between their countries (Roth, 2015). The US-China and the China-Russia agreements are just two of the most recent and visible illustrations of the growing frequency and importance of cyber-diplomacy.

---

[1] Thomas Renard is Senior Research Fellow at the Egmont Institute. Address: 15 rue des petits carmes, 1000 Brussels, Belgium. Email: t.renard@egmontinstitute.be

[2] In a September 2015 statement to the House Permanent Select Committee on Intelligence, US Director of National Intelligence James Clapper identified these countries as the main threats against US cyber security, pointing to a number of known attacks, such as the North Korean attack against Sony or cases of Chinese hacking and espionage. The full statement is accessible online: http://docs.house.gov/meetings/IG/IG00/20150910/103797/HHRG-114-IG00-Wstate-ClapperJ-20150910.PDF

[3] Stuxnet was a highly complex malicious programme, presumably developed by the US, in order to slow down the Iranian nuclear programme. It was launched in 2009 and discovered in 2010. For an account of Stuxnet, you can read Kim Zetter's *Countdown to Zero Day* (Crown, 2014).

Like the rest of the world, the European Union (EU) has become a growing diplomatic actor on cyber issues. Firstly, because these issues were perceived as a threat to Europe's security and prosperity. European member states have been major targets for cyber-crime, cyber-attacks and cyber-espionage. Even the European Union (EU) institutions themselves have been the target of cyber-espionage and cyber-attacks. For instance, a breach in its Emissions Trading System (ETS), the largest carbon-trading scheme in the world, resulted in a loss of around €30 million worth of carbon allowances in 2011 (House of Lords, 2011, p. 39). Secondly, the EU became increasingly active on cyber issues internationally as part of its own integration process, through which the EU is gradually developing itself as a global diplomatic actor and, as a result, cannot ignore a topic of such international prominence.

The EU's first acts of cyber-diplomacy go back to the early 1990s, when the European Commission took part in the international debates on internet governance. It followed with interest the establishment of the Internet Corporation for Assigned Names and Numbers (ICANN), which is today's most important web regulator, and advocated successfully for a greater role for non-US governement in the governance of the internet, resulting in the creation of the Government Advisory Council (GAC) in which the European Commission and EU member states were represented (Christou and Simpson, 2007).

Progressively, the EU has broadened its policy scope to cover cyber-security issues, and to mainstream them in its diplomacy, in a natural extension of its 'domestic' cyber-agenda to the international arena. As a result, the importance of cyber issues was recognized in a number of EU documents, and it was recognized as a strategic challenge in the 2008 implementation report of the European Security Strategy (Council of the EU, 2008). The recent debates leading to the new EU global strategy, adopted in 2016, have further underscored the rising importance of cyber issues to the EU's security (EEAS, 2015a). Therefore, these issues should become ever more important to the EU's global diplomatic efforts.

The EU's cyber-security strategy, published in 2013, was a milestone in the development of the EU's cyber-diplomacy. It sets the promotion of an EU 'coherent international cyberspace policy' as one of its five key priorities (European Commission and High Representative, 2013). The objectives are stated clearly, relating to governance, security and capacity-building: 'the EU will seek to promote openness and freedom of the Internet, encourage efforts to develop norms of behaviour and apply existing international laws in cyberspace. The EU will also work towards closing the digital divide, and will actively participate in international efforts to build cybersecurity capacity' (*Idem*, p.15).

To pursue these objectives, the strategy says, the EU will mainstream cyberspace issues in its external relations and in its Common Foreign and Security Policy (CFSP). In other words, cyber issues are set to become a key topic of the EU's global diplomacy. This cyber-diplomacy, the strategy continues, should be pursued through 'increased engagement and stronger relations with key international partners and organisations', including multilateral and regional organisations as well as third countries. Illustrating this new priority, the leaders of the EU and South Korea 'emphasized the importance of ensuring the openness and security of cyberspace' and 'agreed to increase bilateral cooperation on cyberspace as well as to strengthen the global partnership in response to threats arising from cyberspace' on the

occasion of their latest Summit, in September 2015 (EU-ROK, 2015). Such statement has become relatively common in joint statements with key partners, over the past few years.[4]

This article focuses on the EU's cyber-diplomacy, with a focus on its bilateral dimension. Cyber diplomacy is defined as the use of traditional diplomatic tools to address global cyber issues, such as cyber-crime, cyber-security, cyber-defence and internet governance. It can be located in a broader category called 'digital diplomacy', which goes beyond the substance of diplomacy, to include the new digital instruments of diplomacy (Hocking and Melissen, 2015). Whereas some authors have looked into the EU's cyber-security policies, internally and externally (Sliwinski, 2014) or into the multilateral and governance dimensions of these policies (see for instance Christou and Simpson, 2011), the EU's efforts to engage bilaterally with key cyber powers have remained largely unnoticed. This article connects these bilateral engagements with the broader EU efforts to engage more systematically and strategically with a number of pivotal states, in the framework of the so-called 'strategic partnerships'.

The main argument advanced here is that the EU has started to develop a network of bilateral cyber-partnerships with key countries, which is proving a necessary and useful instrument to pursue the objectives set by its cyber-strategy in a policy field that is contested and largely under-regulated. Furthermore, I argue that these partnerships do not only fulfil bilateral objectives – as the word 'partnership' implies – but they also contribute to other strategic objectives, namely the strengthening of the EU's own diplomatic and cyber agency and the promotion of global norms for the cyberspace.

This article first sets cyber diplomacy and cyber partnerships in the broader context of the emergence of the EU as a global actor and its attempts to develop so-called 'strategic partnerships' with other global powers. It then moves on to identify the specific purposes of these cyber partnerships, and the underpinning mechanisms that support them. Finally, the article explores concrete examples of the cyber partnerships in action, before drawing some conclusions.

2. The EU's partnership diplomacy

In 2003, the European Council adopted the European Security Strategy (ESS), a key policy document aimed at guiding the EU's external action (Council of the EU, 2003). The ESS identified a number of key foreign policy objectives, and proposed to pursue them 'through multilateral cooperation in international organisations and through partnerships with key actors' (Council of the EU, 2003, p.13).

Since 2003, a number of new partnerships were established, mostly with emerging powers. By the end of 2010, the EU had reached a network of 10 strategic partnerships, namely: Brazil, Canada, China, India, Japan, Mexico, Russia (which is currently in limbo, following the Ukrainian crisis), South Africa, South Korea and the USA. After this first phase, the EU decided to shift its efforts from 'widening' (i.e. establishing more partnerships) to 'deepening' (i.e. consolidating existing ones). This second phase was driven internally by a willingness to better define the strategic objectives and scope of each partnership but also, at the bilateral level, to aim for more tangible results (Renard, 2011). Strategic partnerships had become a new foreign policy instrument in the EU's toolbox, inspired by a broader diplomatic trend that

[4] There was, for instance, a full section on cyber issues in the G7 Foreign Ministers Meeting in Lübeck, Germany, 15 April 2015.

saw a proliferation of such partnerships among great and emerging powers, starting in the 1990s (Costa Vaz, 2014; Hamilton, 2014; Zhongping and Huang, 2014).

As foreign policy instruments, strategic partnerships fulfil multiple purposes. Following the work of Grevi (2012) on strategic partnerships and that of Smith, Keukeleire and Vanhoonacker (2016) on strategic and structural diplomacy, three levels of purposes can be identified: reflexive, relational and structural. At the reflexive level, strategic partnerships fulfil both an 'integrative' function and a 'positional' one. Strategic partnerships are 'integrative' in the sense that they provide a narrative that encourages more coherence and cohesion in the EU's foreign policy, thus one that favours more integration and the building of a European identity. Such role is largely supported by the literature on EU global 'actorness' and foreign policy 'identity' (Bretherton and Vogler, 2006; Risse, 2012). Strategic partnerships are also 'positional' as they seek to affirm the EU's role as a global player, in line with the level of ambition set in the ESS, and to assert the EU as an unavoidable interlocutor for the management of key international issues. It is thus essentially a matter of global 'status' and recognition.

At the relational level, strategic partnerships can be seen as a 'means of managing relationships with key partners or in key issue areas which are important to the international life of the Union' (Smith, Keukeleire and Vanhoonacker, 2016, p.5). Since the EU cannot solve global problems on its own, as the ESS recognized, it must address these global challenges in cooperation with key countries, on the basis of mutual interests and benefits. These partnerships are meant to be comprehensive, and to tackle strategic issues – thus going beyond mere economic and diplomatic ties. The relational level is probably the most salient dimension of any partnership, since it relates to bilateral cooperation, but not necessarily the most evident one. Some partnerships focus less on concrete outcomes than on confidence-building mechanisms and socializing processes, due to a lack of trust or inherent tensions to the partnership. Clearly, in some cases, strategic partnerships can be seen as a form of socialization, where the main interest of engagement lies in the process more than in specific goals (Ba, 2006).

At the structural level, bilateral partnerships can be seen as an instrument to promote and shape a more effective multilateral system, as stated in the 2008 revision of the ESS under the label 'partnerships for effective multilateralism' (Council of the EU, 2008). The global multilateral system suffers from a number of problems, relating to legitimacy and effectiveness. Emerging powers are contesting the 'liberal order', in which they are underrepresented, while most countries tend to use multilateralism only selectively (Acharya, 2014). In this context, and given the EU's preference for a strong global governance, bilateral talks with strategic partners can be seen as instruments to strengthen the multilateral fabric (Renard, 2015).

With a view to pursue these different levels of action, EU strategic partnerships are underpinned by a number of documents[5] and dialogues, which together determine the scope and ambition of each partnership. The institutional fabric operating strategic partnerships can vary across relationships, but is overall quite dense.[6] It includes regular meetings at the

[5] Such documents include notably the 'joint action plans' or the more formal 'framework agreements', also known as 'strategic partnership agreements'.

[6] There is overall very limited information available on the dialogues between the EU and third countries, except for scarce and scattered elements on the EU websites, and with a few exceptions. China is one such exception since all dialogues between the EU and China are listed on the website of the European External

highest level, usually annually, as well as ministerial meetings, usually between foreign ministers but sometimes involving other ministers. In addition, there are regular meetings between officials (from senior to technical levels) that cover political issues (such as security matters) and sectoral ones (such as the economy, environment or education, among many others). The EU partnerships with China or the US are underpinned by more than 60 such dialogues, meeting at least once a year but sometimes much more often, whereas the partnerships with South Korea or South Africa are less comprehensive, but still broad-ranging, with over 20 dialogues.

3. Purposes and mechanisms of the EU's cyber partnerships

The EU's cyber diplomacy is not entirely new. As mentioned above, the European Commission has been active in international debates on internet governance, starting as early as the 1990s. However, it is undeniable that the visibility, scope and intensity of this diplomacy has grown significantly over the past few years, largely due to the increasing importance of cyber issues on the international agenda. Emphasizing this new priority, the Council of the EU adopted specific conclusions on cyber diplomacy, in 2015. The conclusions assert that it regards the further development and implementation of a common and comprehensive EU approach for cyber diplomacy at the global level as 'essential and crucial' (Council of the EU, 2015).

These conclusions articulate a vision for the EU's cyber diplomacy, based on the identification of five key priorities: the 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 sixth priority refers less to the *objectives* of cyber-diplomacy, and more to its *channels* as it calls for 'strategic engagement with key partners and international organisations' due to the 'global cross-cutting nature, scope and reach' of cyber issues (Council of the EU, 2015). In practice, this means that the EU has been trying to deepen its ties with a number of key cyber actors, in line with both its growing interest for cyber issues and its broader efforts to engage more strategically at the bilateral level with a number of partners.

The importance of a bilateral approach to cyber issues was already underlined by the European Commission several years ago, emphasising the need for 'strategic cooperation with third countries' to reach a global consensus on internet resilience and stability, or calling for 'a global coordination strategy reaching out to key partners' (European Commission 2009, 2011). Similarly, former European Commissioner for Home Affairs, Cecilia Malmström, said in 2012 that a fundamental objective of the EU's cyber diplomacy is 'to reach out to its strategic partners to make our response more effective' (Malmström 2012). Therefore, when the 2013 Cyber-security Strategy called for a 'renewed emphasis on dialogue with third countries', in order to establish deeper cyber partnerships, it was more a continuation than a revolution in efforts undertaken already in the cyber domain, in line with the broader diplomatic efforts to focus on strategic partners (European Commission and High Representative, 2013).

Action Service (EEAS). However, the European Strategic Partnerships Observatory (ESPO) provides a list of these dialogues with strategic partners, along with additional useful information. Available at: www.strategicpartnerships.eu (last accessed 19 September 2015)

Cyber issues were not originally part of the EU's strategic partnerships. They were not mentioned in the 2003 ESS, which gave way to these new partnerships. However, they later appeared in the 2008 revision of the strategy, and progressively made their way to the partnerships' agenda for cooperation, resulting notably in the establishment of regular meetings and dialogues on these issues, as further explained below. In establishing its cyber partnerships, the EU has therefore been more influenced by its existing partnerships (so-called strategic , than by

With regards to the purposes of cyber partnerships, and cyber diplomacy more broadly, they appear to follow the three levels identified in the previous section. At the reflexive level, cyber partnerships fulfil at least partly an 'integrative' function, as the EU links its cooperation with third countries to the need for greater internal coordination on these issues. Illustrating this, the Council of the EU (2015) encourages the Union and its member states 'to prepare cyber dialogues within the framework of effective policy coordination, avoiding duplication of efforts and taking into account the broader EU political and economic interests, collectively promoted by all EU actors', whereas the cyber strategy insisted that 'EU consultations with international partners on cyber issues should be designed, coordinated and implemented to add value to existing bilateral dialogues between the EU's member states and third countries'. There is also a certain 'positional' function that emerges from the EU's efforts to engage with major cyber powers, and particularly the US, while seeking to establish itself as a leader or, in the Commission's own words, as a 'honest broker' in the debate on internet governance (Christou and Simpson, 2011; European Commission, 2014b).

The relational level is the most basic level of expectation for any partnership. Cyber partnerships pursue relational purposes through the identification of common objectives in various documents or statements, and through the development of specialized dialogues on cyber. Yet, the level of cooperation can vary across partnerships. In fact, one can distinguish between two types of partnerships: *results-oriented* and *process-oriented* ones. Results-oriented partnerships aim for tangible outcomes, such as strengthening their mutual cyber-security or developing joint initiatives. Their value can be therefore assessed against these objectives. Process-oriented partnerships focus instead on the socialization dimension, with the aim to increase mutual knowledge and trust, or at the very least to mitigate tensions and keep the channel of communication open. The value of such partnership is often more difficult to appreciate.

At the structural level, cyber partnerships can play a role in promoting more effective multilateral instruments, notably against cyber-crime. Since the multilateral fabric is particularly thin in this policy area, bilateral cooperation appears necessary to palliate and, eventually, strengthen multilateral instruments. Cyber partnerships can also be tools to shape internet governance. As stated in the Council of the EU's conclusions: 'internet governance is an integral part of the common and comprehensive EU approach for cyber diplomacy' (Council of the EU 2015). Furthermore, internet governance has been described by a number of observers as one of the most important topics of global diplomacy (Kleinwächter, 2008). The European Commission articulated its vision for internet governance on several occasions, lately in a Communication entitled 'Europe's role in shaping the future of internet governance' (European Commission 2014a). In this document, the Commission promotes a number of principles, namely fundamental rights, democratic values and a single, unfragmented network; and it sets key objectives, namely defending the multi-stakeholder model of governance, strengthening a reformed Internet Governace Forum (IGF) and globalising ICANN (thus ending the American stewardship over the internet).

With regard to the institutional aspects of these cyber partnerships, a growing number of dialogues are gradually taking place. Discussions can take place at the highest level, between respective leaders, eventually making its way to the final joint statements. Discussions can also take place at the ministerial level. For instance, cyber-crime has been tackled in the framework of the EU-US justice and home affairs ministerial meeting, which gathers twice a year. The issue has also been addressed occasionally by the EU-Russia Permanent Partnership Council (PPC). Cyber-security has also been discussed between foreign ministers and the EU's High Representative. This has been the case with the US, but also with China and India. During their second High-Level Strategic Dialogue in 2011, the EU and China briefly discussed possibilities to develop their dialogue on cyber-security, eventually leading to the establishment of a taskforce the following year.

At the working level, there are a number of structured dialogues between the EU and its partners. The EU-US partnership is the most developed in this regard, mainly through the Working Group on Cyber-security and Cyber-crime (WGCC), established in 2010. It is articulated around four priority axes: cyber-incident management; public-private partnerships; awareness raising; and combating cyber-crime. There is also an annual Information and Society Dialogue, dealing notably with internet policy and governance. At the latest EU-US summit, in March 2014, a new cyber dialogue was launched to deal with 'cross-cutting cyber issues, key international cyber developments and foreign policy-related cyber issues' (EEAS, 2014). In addition to these bilateral consultations, the transatlantic partnership is reinforced by a trilateral EU-US-Canada expert meeting on critical infrastructure protection, which addresses cyber-threats.

Other partnerships are less developed. An EU-China Cyber Taskforce was established in 2012 to address common cyber threats through 'enhanced bilateral exchanges and cooperation. It will also promote and develop technologies related to information and communication security, with a view to fostering economic and social development' (Pan, 2012, p.3). The EU and India meet annually in the context of the political dialogue on cyber-security, in the context of which they have discussed 'cybersecurity, cybercrime, internet governance, standards and regulation, capacity building and research and development issues from an international policy perspective' (EEAS, 2015b). An EU-Brazil Dialogue on International Cyber Policy, an EU-Japan Cyber Dialogue, as well as a similar dialogue with South Korea were set up in early 2014. The EU-Mexico dialogue on public security and law-enforcement should address cyber-crime, but this has not been the case yet. A number of ICT-related dialogues are in place with some partners, in the framework of which certain issues such as internet governance can be addressed. This includes the information society dialogues with Brazil, India, Russia, South Africa and South Korea, the EU-China dialogue on IT, telecommunications and informatisation, the EU-Japan dialogue on ICT policy, or EU-Mexico Working Group on telecommunications.

4. Cyber partnerships in action

This section reviews in more details how the various cyber partnerships of the EU unfold in practical terms, what objectives they have set and what outcomes they have produced, if any. This empirical overview will then serve as a basis to assess these partnerships and, more broadly, the EU's cyber diplomacy. Four main areas of cooperation are investigated here: exchange of information and best practices on cyber-security, cyber-crime and capacity-

building efforts; agreements to facilitate bilateral exchanges and cooperation on cyber-crime; multilateral instruments against cyber-crime; and discussions on internet governance.

Exchange of information and best practices on cyber-security, cyber-crime and capacity-building efforts

One of the key objectives of cyber partnerships is to improve mutual and global cyber-security. Yet, not all partnerships deliver equally on this front. The EU-US bilateral partnership is by far the oldest and most developed. Some initial forms of cooperation go back to early the 2000s, notably with the EC-US Task Force on Critical Infrastructure Protection, established in 2000. Today, the partnership relies primarily on the WGCC, which identifies clear priority areas for cooperation, as well as concrete deliverables, following a specific roadmap. (EU-US, 2011). The EU has no equivalent dialogue with any other partner. The first priority area identified by the WGCC was cyber incident management. In November 2011, the EU and the US conducted their first joint cyber-security exercise – the first ever with a non-European partner, which closely followed the first pan-European exercise for Critical Information Infrastructure Protection (CIIP).[7] The joint exercise brought together over 100 government experts from both sides to assess responses to cyber-espionage and cyber-attacks. In October 2014, the two sides cooperated to jointly promote a 'cybersecurity awareness raising month' in Europe and in the US.

The WGCC is complemented by two other bilateral structured cyber-dialogues, as well as a series of contacts between relevant actors from both sides. The EU-US partnership is deemed by officials to be 'very operational' and 'very successful' on cyber-crime.[8] The US is also considered a key cooperation partner in science, technology and innovation in relation to cyber security (European Commission, 2012, p.58). The EU-US partnership is perhaps the only one sufficiently advanced to consider triangulated efforts for cyber capacity building in third countries, such as improving access to internet and preventing cyber threats. Discussions for a coordinated approach have been initiated.[9] There is thus a thick network connecting both partners, allowing for broad cooperation, although a certain degree of distrust continues to overshadow the relationship, particularly in the aftermath of the Snowden revelations. The difficulty to conclude the so-called 'Safe Harbour' agreement meant to facilitate the exchange of digital information across the Atlantic is yet another sign of this distrust, which is overall still limiting the scope and depth of cooperation.

Beyond the US, there are numerous contacts with Canada, mainly with regard to cyber-crime and CIIP. The partnership with Canada is still in development, and it is perhaps better seen in the broader transatlantic framework as a complement to the EU-US partnership, rather than as a stand-alone partnership.[10] Cooperation also takes place on cyber-crime with Japan, notably

[7] According to the website of the European Network and Information Security Agency , 'Cyber Europe 2010 was organised by EU Member States, facilitated by ENISA and supported by the Joint Research Centre (JRC). The objective of the exercise was to trigger communication and collaboration between countries in Europe to try to respond to large-scale attacks. During the Cyber Europe 2010 exercise, experts from the participating public bodies of European countries worked together to counter simulated attempts by hackers to paralyse the Internet and critical online services across Europe.' The full report is accessible online: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010/ce2010report

[8] Interview with an EEAS official, Brussels, 16 April 2013; interview by email with an official from the EC3, 8 April 2013.

[9] Interview 16 April 2013, op. cit.

[10] Interview with an official from DG Home, Brussels, 13 May 2013.

through the European Cyber-crime Centre (EC3). Other cyber-security issues, such as CIIP and smartphones security, have been discussed between the European Network and Information Security Agency (ENISA) and a Japanese agency (ENISA, 2011). In 2012, the two partners co-organised a major Internet Security Forum to exchange information 'on policy and technical trends related to ensuring internet security' (MIC, 2012). In addition, the EU and Japan have funded joint research projects on cyber-security. Similarly, the EU and Brazil have unlocked joint funding under their research programmes to address 'internet governance and security' (European Commission, 2011).

Bilateral cooperation between the EU and Russia, or China, is less straightforward. These two countries are perceived as major sources of cyber-attacks and cyber-espionage in Europe. As mutual trust is lacking, cooperation focuses mostly on confidence-building measures. This is one of the key aims of the EU-China cyber taskforce, even though the discussions around the modalities of the taskforce were rather difficult, reflecting the deep rift between the two partners (Sénat de Belgique, 2012). The EU also supports China in the development of data protection laws (Pawlak and Sheahan, 2014). More cooperation is foreseen in the future, as expressed in the EU-China 2020 Strategic Agenda for Cooperation, notably on cyber-crime (EU-China, 2013). With Russia, cooperation first focussed on the use of internet by terrorist groups and has gradually expanded to cover cyber-crime. Some operational cooperation on cyber-crime has been reported by the EC3 since its launch.[11] More cooperation has been considered on cyber-terrorism, namely through Russian participation in Europol's 'check the web' initiative, which monitors terrorist websites, as well as on cyber-crime, namely through the exchange of information on harmful viruses used by cyber-criminals. (Hernandez i Sagrera and Potemkina, 2013). Overall, however, cooperation remains very limited and the Ukrainian crisis is clearly exacerbating tensions between the two parties.

With the rest of strategic partners very little bilateral cooperation has been reported, in spite of existing dialogues. India is perceived as a 'promising partner', according to an EU official, but the policy dialogue has yielded few results so far.[12] The same applies to South Korea. As for Mexico and South Africa, no cooperation on cyber-security was reported, despite the bilateral dialogues on crime and ICT.

Agreements to facilitate bilateral exchanges and cooperation on cyber-crime

The cyber-sphere is sometimes perceived as borderless. However, it is not so much physical borders that have disappeared. Instead, it is the combination of absent virtual borders with existing and distinct legal ones that has allowed for cyber-offences to thrive. The coordination of legal frameworks on cyber-security and the conclusion of operational agreements with partners are particularly important in this context.

There are two kinds of bilateral agreements that can be concluded between the EU and its strategic partners with a view to facilitating cooperation against cyber-crime: first, legal acts related to cooperation on criminal justice or law-enforcement; and second, operational agreements to allow for exchanges and cooperation between operational agencies.

Agreements on extradition and mutual legal assistance (MLA) fall in the first category. They are deemed important for they facilitate cooperation in the course of (cyber-)criminal investigations. MLAs also facilitate the setting up of joint investigations teams. The 2003 EU-

[11] Interview 8 April 2013, op. cit.
[12] Interview 16 April 2013, op. cit.

US extradition and MLA agreements, which entered into force in 2010, were the first justice and home affairs international agreements signed by the EU. Japan is the only other strategic partner with whom the EU has signed an MLA agreement, in 2009. The possibility of starting MLA negotiations with India or Russia has been mentioned several times, but this has been hampered by a lack of political will and trust.

The second category of operational agreements has been described as a 'sub-category' of bilateral agreements (Mönar, 2012, p.58). It includes agreements concluded between EU agencies and partner countries. The number of such agreements has been steadily increasing, but their scope remains limited. Europol has concluded an operational agreement with ten countries, including Canada and the US. As a result, the EU and its partners can share highly-sensitive information. Such cooperation is usually complemented with an exchange of liaison officers to facilitate information sharing. Europol also signs 'strategic agreements', but these do not have the same level of confidentiality and thus inhibit the exchange of sensitive data. Europol has concluded eight such agreements, including with Russia. There are regular experts meetings with Russia in Europol, and a decision was taken to establish a cyber-crime platform in Europol that would permanently include Russian experts.[13] In 2009, the Council of the EU mandated Europol to start negotiating an operational agreement with Russia to deepen cooperation, although the negotiation of this agreement is now on hold (Council of the EU, 2009). Agreements with India and China have been considered but negotiations have been postponed, preventing cooperation. In some cases, the lack of an agreement has not entirely hindered constructive cooperation, as is the case with Japan.

Eurojust has concluded six agreements with third countries, including the US. A cooperation agreement has been under negotiation for years with Russia, but it has not yet been concluded and it is currently on hold. In the absence of an agreement, contacts and exchanges can nonetheless take place between Eurojust and the EU's strategic partners. Contacts have been established with the Russian Office of the General Prosecutor, and cooperation has led to some confidence building exercises such as a joint seminar on judicial cooperation in 2009 (Eurojust, 2010). A bilateral working group was also set-up in 2011 with a view to solving practical problems related to cooperation in criminal matters. Liaison magistrates are in place with Japan and South Korea. Contacts also exist with India, as well as with Canada through its counsellor of international criminal operations, based in the mission to the EU since 2002.

Strengthening multilateral instruments

Bilateral cooperation is not sufficient to cope with a global challenge such as cyber-security. The crafting of collective efforts and multilateral instruments in this area has become a major priority over the last years worldwide. The need for multilateral cooperation is enshrined in the EU's Cyber-security Strategy. It puts a particular emphasis on the Council of Europe's Budapest Convention.

The Budapest Convention is the only binding international agreement on cyber-security, focussing on cyber-crime. It facilitates operational cooperation and sets guidelines for developing and harmonising the different national legal frameworks. There is a general agreement in Europe that this convention 'represents a major advance toward creating a common judicial area' in cyber-issues (Bendiek, 2014, p.10). The Budapest Convention is open to third countries, beyond the members of the Council of Europe, and the EU has

[13] Interview with a Russian diplomat, Brussels, 31 May 2011.

actively sought to promote it. It is therefore a useful instrument for the global promotion of European norms. Indeed, the signature or broad acceptance of the convention is seen by the EU as an essential condition to provide financial support for cyber capacity-building in a third country.[14]

The US, Canada and Japan have signed and ratified the convention, which they also helped drafting as observer states (together with South Africa as well). The EU-US partnership is unique in this regard, since both sides are committed to jointly promoting the convention and to attracting an even broader group of nations to become parties, as stated in the WGCC concept paper (EU-US, 2011). South Africa has signed but not ratified it, and Mexico's signature is still pending. Among the opponents to the convention, Russia and China lead the charge. Russia stands out, however, as a member of the Council of Europe – the only one among the EU's partners. Views have been exchanged to address Russia's objections, although a convergence of views is now even less likely given the suspension of Russia's voting rights in the Parliamentary Assembly of the Council of Europe as a result of its annexation of Crimea. The positions of Brazil and India are more nuanced. They do not fundamentally contest the convention and they even arguably used it as a guideline for reforming their national legislation. Yet, they do not support it either, perhaps because they were not involved in the drafting process, or because they see it as a too 'Western' initiative.

The Global Alliance against Child Sexual Abuse Online is another important international instrument against cyber-crime, although non-legally binding and more limited in scope. This political initiative aims at fighting child sexual abuse online, identifying, protecting and supporting victims, reducing availability of child pornography, prosecuting offenders and raising awareness. It was launched jointly by the EU and the US in 2012, and now brings together 53 countries including four additional EU strategic partners, namely Canada, Japan, Mexico and South Korea.

Beyond these international instruments, a number of multilateral organisations have proven useful in developing or coordinating cyber-security policies. In the framework of the UNODC expert group on cyber-crime, the EU and the US regularly coordinate positions. The G7/8 has also been active in cyber-security, setting up a sub-group on high-tech crime in which the EU is an observer. This sub-group has the ambition to draft guidelines and provide training beyond the small group of G8 members. A network of contact points has been established for relevant transnational investigations, including contact points from all strategic partners except China, available 24 hours a day, 7 days a week. The OECD and the OSCE are two other relevant organisations, which have developed initiatives on cyber-security. The EU has actively supported the establishment of confidence building measures with Russia, in the framework of the OSCE, and with China and other Asian countries, in the framework of the ASEAN Regional Forum (ARF) (European Commission, 2014c). The so-called 'London Process' is yet another platform for discussing cyber issues. Initiated by former UK Foreign Secretary William Hague in 2011, it has convened international leaders annually in order to generate a consensus on responsible behaviour in cyber-space.

Finally, NATO has become a major actor in cyber-security, focussing essentially on cyber-defence. In this context, Europeans have been able to bolster their capabilities, in coordination with the US and Canada. Since 2010 there have been regular EU-NATO informal staff-to-staff meetings on cyber-security. Areas for cooperation have been identified, including raising

[14] Interview 16 April 2013, op. cit.

cyber-security awareness, joint trainings, and developing capabilities in terms of cyber-resilience. Cyber-security was also discussed with Russia in the past, in the framework of the NATO-Russia Council.

Shaping internet governance

The broader question of internet governance appears to be a particularly contentious and divisive issue internationally. Currently, internet governance is not based on traditional multilateralism, but rather on a multi-stakeholder system involving governments as well as businesses, civil society actors and technical experts. Its regulatory decisions are based on loose consensus rather than rigid voting procedures. A major institution in the policy governance of the internet is the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for 'three of the most vital functions of the internet' (Klimburg and Tiirma-Klaar, 2011, p.21): allocating IP addresses, DNS names and Top Level Domains (TLD). Although this might sound highly technical, the consequences are in fact highly political: if governments were to control these functions more strictly, they would significantly increase their ability to block certain websites, content or users.

There are essentially two main opposing models of internet governance. On the one side, there are those states that support a multi-stakeholder model and the work of ICANN, with a view to maintaining an open, accessible, dynamic and private internet. The EU, the US, Canada and Japan belong to this group. On the other hand, some states, particularly authoritarian ones, push for an inter-governmental model, in which national governments have greater control over the internet. They support an internet global *government*, rather than governance, with a greater role for the International Telecommunication Union (ITU), a United Nations agency, which could gradually replace ICANN. Russia and China belong to this group.

Although the EU and the US jointly support the multi-stakeholder model, they have never been fully aligned (Christou and Simpson, 2011). They had different visions from the beginning, which eventually led to hard compromises, but never to confrontation. The revelations of former NSA consultant Edward Snowden, unveiling of a massive American spying operation on US allies, have revived these divergences. The EU has openly challenged US government influence over ICANN and its department on the Internet Assigned Numbers Authority (IANA), since it is accountable to the US Department of Commerce in certain areas – a powerful right to 'hide' certain websites, although allegedly never used. In a 2014 statement, the European Commission called for a more 'transparent, accountable and inclusive' internet governance, referring specifically to the 'large-scale internet surveillance' by the US and the resulting 'reduced trust in the internet' (European Commission, 2014b). Overall, the EU does not challenge the bottom-up multi-stakeholder approach, but rather the US stewardship and the US-centric model of internet governance, not least since internet usage has significantly globalised over the last decade. More than half of internet users worldwide are now in Asia. In March 2014, the US Department of Commerce announced that it would give up its control over ICANN, and the EU and the US discussed the future of internet governance during their latest summit the same month.

The other multilateral governance context that is central to the EU's cyber diplomacy is the Internet Governance Forum (IGF), which is also a multi-stakeholder body that emerged from the World Summit on Information Society (WSIS), conducted in two phases between 2003 and 2005 (European Commission, 2014a). Similarly to the ICANN's situation, the EU and the

US have mild divergence of views, which has somehow forced the EU into a position of 'mediator' between the US and many other countries (Christou and Simpson, 2011, p.250). Therefore, in the context of internet governance, the US is a close partner of the EU, but also a challenging one. As the EU attempts to promote its own normative preferences, it may soon seek to deepen some of its cyber partnerships with 'like-minded' countries. A recent study on internet governance identified 30 potential swing states that could play a pivotal role in this debate (Maurer and Morgus, 2014). Five EU strategic partners figure in this list: Brazil, India, Mexico, South Africa and South Korea.

5. EU cyber partnerships: More than meet the eye

Cyber issues have long been marginal to the EU's international diplomacy. When most EU strategic partnerships were established, there was little or no mention of cyber-security issues in the agenda for cooperation. The 2001 EU-Japan Action Plan, the 2005 EU-Russia Common Spaces Roadmap, the 2005 EU-India Joint Action Plan (and its update), the 2010 EU-Mexico Joint Executive Plan and the 2010 EU-South Korea Framework Agreement make only brief references to cyber-security; whereas the 1995 EU-US New Transatlantic Agenda, the 2004 EU-Canada Partnership Agenda, the 2006 EU-South Africa Joint Action Plan and the 2008 EU-Brazil Joint Action Plan make no reference at all to cyber issues. Furthermore, in contrast to what has occurred in the case of other security challenges, such as terrorism or nuclear proliferation, the EU has never adopted a joint statement specifically focussed on cyber issues with its partners.

Arguably, cyber issues were not very much at the centre of international diplomacy either. Things are changing, however. Cyber-security and internet governance have gained global traction in recent years, and they are likely to become more prominent in the EU's diplomatic efforts, as well as in its strategic partnerships. Many of the above-mentioned documents are outdated and some are undergoing revision. The EU-China 2020 Strategic Agenda for Cooperation, which addresses cyber issues, arguably confirms this; and the EU and Brazil announced at their latest summit that cyber-security and internet governance will be part of their next joint action plan (EU-Brazil, 2014). The EU-Canada Strategic Partnership Agreement (SPA), concluded in 2014 but still to be ratified, also includes an article that encourages further cooperation on cybercrime (EU-Canada, 2014).

The recent multiplication of bilateral dialogues with partners confirms the rising importance of this topic in the partnerships' agenda. Four new dialogues were launched in 2014 – with Brazil, Japan, South Korea and the US. There is now at least one dialogue on cyber-related issues with each of the EU's ten strategic partners. Although some of these dialogues are rather technical (on ICT or on crime more broadly), the inevitable trend is that of a quickly thickening fabric of the EU's cyber-diplomacy.

In short, the EU cyber partnerships are still work in progress. As a result, their ability to fulfil strategic purposes remains somewhat limited. In order to assess the strategic value of these partnerships, I will now refer back to the three levels of purposes detailed earlier in this article. At the reflexive level, some partnerships have arguably played in favour of the 'integrative' function, particularly the most challenging ones. The multiple acts of cyber-espionage and cyber-offences from major powers – mostly the US, Russia and China – strengthen the EU's argument for stronger national capabilities and for more coordination on cyber issues. Various aspects of the cyber-agenda have been raised at the European level following such attacks, a number of measures have been taken to improve national and

European capabilities, and cyber exercises have been organised to improve Europe's overall response to cyber incidents. Nevertheless, surprisingly, the EU institutions and member states have largely refrained from publicly pointing fingers at the attackers, beyond a few statements, even when the offence was publicly recognized, as in the case of the US spying programme (Dworkin, 2015). The 'integrative' function of cyber partnerships is thus essentially latent, and limited by the EU's member states prerogatives on security matters.

Cyber-partnerships appear to perform better on the 'positional' function, at first. By establishing cyber dialogues with all its ten strategic partners, the Union has managed to assert itself as a worthwhile interlocutor in the cyber domain. All these cyber partnerships create a network, in which the EU is a hub – among several others. However, the 'positional' function of cyber partnerships is largely related to the 'integrative' one. As noted by the former European Commissioner for a Digital Agenda, Neelie Kroes (2013), a common European approach would allow the EU to become a more strategic and trusted international partner at the international level. But since the EU remains still a fledgling cyber agent, and perceived as such by other global cyber powers, the 'positional' function of these cyber partnerships remains partial, albeit progressing.

At the relational level, all cyber partnerships are neither equal, nor identical. The transatlantic partnership is by far the most developed, institutionally as well as in terms of tangible cooperation. It is also the only partnership aiming for 'global rule-making objectives' (Fahey, 2014, p.21) in line with the joint decision to raise the issue to the level of 'global concern' in 2009 (EU-US 2009). Above all, it is the only partnership singled out in the EU's cyber strategy. All the other partnerships are less developed institutionally and less ambitious in scope, in spite of the strategy's call to deepen cooperation with 'like-minded partners that share EU values'. Signs of cooperation arise occasionally, but most cyber partnerships remain largely under-delivering.

Such observation would fundamentally challenge the notion of cyber partnership, if it were not for the distinction between *results-oriented* and *process-oriented* partnerships. Whereas the transatlantic partnership aims for tangible deliverables, such as increasing cyber-security in the transatlantic space and beyond, the partnerships with China and Russia seek mostly to keeping the dialogue open on contentious issues, and possibly aim to building mutual confidence. Having said this, most cyber partnerships operate eventually a balance between results and process. Even the EU-US partnership seeks to strike this balance, as it is still hampered by a serious trust-deficit.

At the structural level, cyber partnerships have proven particularly useful in the context of international discussions on the internet governance. The EU and its 'like-minded' partners defend a certain vision of the internet, which is opposed by some other partners. Although the EU cannot be considered a 'honest broker' in this debate, being an active protagonist, it deploys nonetheless active diplomacy to reach out an acceptable solution for all parties. Cyber partnerships have also been necessary to cope with thin multilateralism. The EU has not only actively promoted the Budapest Convention vis-à-vis, or together with its partners, but it has also launched new initiatives with some of them, namely the Global Alliance against Child Sexual Abuse Online.

6. Conclusion

The EU's interest for cyber issues is not new, but it has been significantly boosted over the past few years, as these issues have been progressively considered to be 'strategic'. The EU's cyber diplomacy has developed accordingly, mirroring both a global trend and the development of the EU as a diplomatic actor. However, cyber issues are still not the most visible part of the EU's global diplomatic efforts. After all, the EU is both a fledgling cyber-security and diplomatic agent. Most EU efforts are thus still inward-looking, focussing on the need to increase European capabilities and coordinate more actions. However, internal *coordination* cannot be entirely dissociated from international *cooperation*, as the cyber challenge is not just a European one, but a global one.

In order to facilitate and deepen such cooperation, the EU has developed a number of cyber partnerships with key countries. At first sight, these partnerships appear very unsatisfactory, since they deliver little results. Some partnerships are even doubtful, since they involve countries that are more source of cyber insecurity than of cyber security. Yet, this article has argued that these partnerships can be helpful in more than one way, for instance by building trust among partners and thus laying the foundations for future cooperation, at the bilateral and multilateral levels. Moreover, cyber partnerships fulfil a number of other purposes, such as identity building and the assertion of global status, as well as the strengthening of global governance. It is noteworthy that these various levels of purposes are all related to one another. As pointed out in this article, the EU-US partnership has a significant 'global' dimension, as it seeks to shape global rule-making, but it also has a major influence on the EU's own internal priorities and rule-making, as confirmed by Fahey (2014).

The value of cyber partnerships can only be measured against these multiple and complex purposes. Every partnership fulfils each purpose to some extent, although significant variations exist and distinguish the relative importance of each individual partnership. But it is the EU's network of cyber partnerships overall that contributes the most to these purposes, particularly – and perhaps counter-intuitively the most – to the reflexive level. In light of this multi-level analysis, this article concludes that cyber partnerships are not only a growingly essential part of the EU's cyber-diplomacy, but also more broadly of its own diplomatic and cyber agency.

References

Acharya, A. (2014) *The end of American world order*, Cambridge: Polity Press.

Ba, A.D. (2006) 'Who's socializing whom? Complex engagement in Sino-ASEAN relations', *The Pacific Review*, 19(2), pp. 157-79.

Bendiek, A. (2014) 'Tests of partnership: Transatlantic cooperation in cyber security, internet governance and data protection', Research Paper 5, Berlin: Stiftung Wissenschaft und Politik.

Bretherton, C. and J. Vogler, (2006) *The European Union as a Global Actor*, London: Routledge.

Christou, G. and S. Simpson, (2007) 'Gaining a stake in global internet governance: the EU, ICANN and strategic norm manipulation', *European Journal of Communication*, 22(2), pp. 147-65.

Christou G. and S. Simpson, (2011), 'The European Union, multilateralism and the global governance of the internet', *Journal of European Public Policy*, 18(2), pp. 241-57.

Costa Vaz, A. (2014) 'Brazil's strategic partnerships: origins, agendas and outcomes', ESPO Working Paper 9, Brussels: European Strategic Partnerships Observatory (ESPO).

Council of the EU, (2003) 'A secure Europe in a better world: European Security Strategy', December 2003.

Council of the EU, (2008) 'Providing security in a changing world: Report on the implementation of the ESS', December 2008.

Council of the EU, (2009) 'Press release of the 2936th Council meeting on Justice and Home Affairs', Luxembourg, 6 April 2009. Available online at: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/107164.pdf

Council of the EU, (2015) 'Council conclusions on cyber diplomacy', Brussels, 11 February 2015.

Dworkin, A. (2015) 'Surveillance, privacy, and security: Europe's confused response to Snowden', ECFR Policy Memo, London: European Council on Foreign Relations (ECFR).

EEAS, (2014) 'EU-US cooperation on cyber security and cyberspace', Fact Sheet. Available online at: http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf

EEAS, (2015) 'The European Union in a changing global environment: A more connected, contested and complex world', Report, 30 June 2015.

EEAS, (2015) 'EU and India Cyber Dialogue', Press Release, 22 May 2015.

ENISA, (2011) 'ENISA hosting the Japanese Information-technology Promotion Agency, "IPA"', Press Release, 15 December.

Eurojust (2010) 'Annual Report 2009', The Hague: Eurojust.

European Commission, (2009) 'Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 30 March 2009.

European Commission, (2011) 'Digital Agenda: EU and Brazil strengthen ties with €10 million joint ICT field research programme', Press Release, Available online at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1316

European Commission, (2012) 'ICT research and innovation in a globalised world', ISTAG Working Group on International Cooperation, Brussels: European Commission.

European Commission, (2014) 'Internet Policy and Governance: Europe's role in shaping the future of Internet Governance', Communication from the commission to the European

parliament, the council, the European economic and social committee and the committee of the region, 12 February 2014.

European Commission, (2014) 'Commission to pursue role as honest broker in future global negotiations on Internet Governance', Press Release, 12 February 2014. Available online at: http://europa.eu/rapid/press-release_IP-14-142_en.htm

European Commission, (2014) 'Table on the Implementation of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"', Working document, 28 February 2014.

European Commission and High Representative, (2013) 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions, 7 February 2013.

EU-Brazil, (2014) 'Joint Statement', 7th EU-Brazil Summit, Brussels, 24 February 2014. Available online at: http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/141145.pdf.

EU-Canada, (2014**) '**Strategic Partnership Agreement between the European Union and its Member States, of the one part, and Canada, of the other part', Text to be ratified.

EU-China, (2013), 'EU-China 2020 Strategic Agenda for Cooperation'. Available online at: http://eeas.europa.eu/china/docs/eu-china_2020_strategic_agenda_en.pdf

EU-ROK, (2015) 'Joint Press Statement', 8th Republic of Korea-EU Summit, Seoul, 15 September 2015.

EU-US, (2009) 'Summit declaration', 3 November 2009. Available online at: http://www.eeas.europa.eu/us/sum11_09/docs/declaration_en.pdf

EU-US, (2011) 'Concept Paper', EU-US Working Group on Cyber-security and Cyber-crime.

Fahey, E. (2014) 'The EU's cybercrime and cybersecurity rule-making: mapping the internal and external dimensions of eu security', Working Paper Series 02, Amsterdam: Amsterdam Centre for European Law and Governance.

Grevi, G. (2012) 'Why EU strategic partnerships matter,' ESPO Working Paper 1, Brussels: European Strategic Partnerships Observatory (ESPO).

Hamilton, D. (2014) 'The American way of partnership', ESPO Working Paper 6, Brussels: European Strategic Partnerships Observatory (ESPO).

Hocking, B. and J. Melissen, (2015) 'Diplomacy in the digital age', The Hague: Clingendael Institute.

House of Lords, (2011), 'The EU internal security strategy', Report, 17th Report of Session 2010–12.

Kleinwächter, W. (2008) 'Multi-stakeholder internet governance: the role of governments', in W. Benedek, V. Bauer and M.C. Ketteman (eds), *Internet governance and the information society: Global perspectives and European dimensions*, Utrecht: Eleven International, pp. 9-29.

Klimburg, A. and H. Tiirmaa-Klaar, (2011) 'Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU', European Parliament Study, Brussels: European Parliament.

Kroes, N. (2013) 'Towards a coherent international cyberspace policy for the EU', Speech at the Global Cyber Security Conference, Brussels, 30 January 2013.

Malmström, C. (2012) 'The European Response to the rising Cyber Threat', Speech at the Transatlantic Cyber Conference, Washington. 2 May 2012.

Maurer, T. and R. Morgus, (2014) 'Tipping the scale: an analysis of global swing states in the internet governance debate', Internet Governance Papers 7, Waterloo: CIGI.

MIC, (2012) 'Outcome of 19th Japan-EU ICT dialogue and Japan-EU Internet Security Forum', Ministry of Internal Affairs and Communication (MIC) News.

Mönar, J. (2012) 'The external dimension of the EU's area of freedom, security and justice: Progress, potential and limitations after the Treaty of Lisbon', Report 1, Stockholm: Swedish Institute for European Policy Studies.

Nakashima, E. and S. Mufson (2015) 'U.S., China vow not to engage in economic cyberespionage', *The Washington Post*, 25 September. Available online: https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html

Pan, Z. (2012) 'After the China-EU summit: reaffirming a comprehensive strategic partnership', ESPO Policy Brief 3, Brussels: European Strategic Partnerships Observatory (ESPO).

Pawlak, P. and C. Sheahan, (2014) 'The EU and its (cyber) partnerships', Brief Issue 9, Paris: EU Institute for Security Studies.

Hernandez i Sagrera, R. and O. Potemkina, (2013) 'Russia and the Common Space on Freedom, Security and Justice', CEPS Paper in Liberty and Security in Europe 54, Brussels: Centre for European Policy Studies (CEPS).

Renard, T. (2011) 'The treachery of strategies: A call for true EU strategic partnerships', Egmont Paper 45, Brussels: Egmont Institute.

Renard, T. (2015) 'Partnerships for effective multilateralism? Assessing the compatibility between EU bilateralism, (inter-)regionalism and multilateralism', *Cambridge Review of International Affairs*, forthcoming issue, online (DOI: 10.1080/09557571.2015.1060691).

Risse, T. (2012) 'Identity Matters: Exploring the Ambivalence of EU Foreign Policy', *Global Policy*, 3(1), pp. 87-95.

Roth, A. (2015), 'Russia and China sign Cooperation Pacts', *New York Times*, 8 May 2015. Available at: http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0

Sénat de Belgique, (2012) 'Question écrite n° 5-6135', 24 April 2012. Available online at: http://www.senate.be/www/?MIval=/Vragen/SVPrintNLFR&LEG=5&NR=6135&LANG=nl

Sliwinski, K.F., (2014) 'Moving beyond the European Union's weakness as a cyber-security agent', *Contemporary Security Policy*, 35(3), pp. 468-86.

Smith, M.H., Keukeleire, S. and S. Vanhoonacker, (2016) 'Introduction', in M.H. Smith, S. Keukeleire and S. Vanhoonacker (eds), *The diplomatic system of the European Union: Evolution, change and challenges*, Abingdon: Routledge, pp. 1-8.

Zhongping, F. and J. Huang, (2014) 'China's strategic partnership diplomacy: engaging with a changing world', ESPO Working Paper 8, Brussels: European Strategic Partnerships Observatory (ESPO).