

Accepted Manuscript (AM) version.

Please note that there are some minor differences with the final published manuscript.



European Politics and Society



ISSN: 2374-5118 (Print) 2374-5126 (Online) Journal homepage: <http://www.tandfonline.com/loi/rpep21>

EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain

Thomas Renard

To cite this article: Thomas Renard (2018): EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain, European Politics and Society, DOI: [10.1080/23745118.2018.1430720](https://doi.org/10.1080/23745118.2018.1430720)

To link to this article: <https://doi.org/10.1080/23745118.2018.1430720>



Published online: 29 Jan 2018.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

Full Terms & Conditions of access and use can be found at
<http://www.tandfonline.com/action/journalInformation?journalCode=rpep21>

EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain

THOMAS RENARD¹

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

¹ Thomas Renard is Senior Research Fellow at the Egmont Institute, and Adjunct Professor at the Vesalius College, Brussels. 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-Clapper-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).

are just two of the most recent and visible illustrations of the growing frequency and importance of cyber-diplomacy.

Like the rest of the world, the European Union (EU) has become increasingly interested in 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 acquaintance with cyberspace go back to the early 1990s, when the European Commission took part in the international debates on internet governance. Progressively, the EU has broadened its policy scope to cover various aspects of cyber-security, and to mainstream them in its external relations, 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. It was recognized as a strategic challenge in the 2008 implementation report of the European Security Strategy (Council of the EU, 2008), whereas an EU cybersecurity strategy was adopted in 2013 (European Commission and High Representative, 2013). The recent EU global strategy, adopted in 2016, further confirmed the rising importance of cyber issues to the EU's security agenda (EEAS, 2016).

There have been a growing number of articles on the EU's cyber policies over the past years. Some authors have for instance 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). However, the EU's efforts to engage bilaterally with key cyber powers have remained largely unnoticed and understudied. This article seeks to address this gap, with a view to better understand the ambition and behaviour of the EU as an international cyber actor. It does so by connecting these bilateral cyber partnerships 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 research question underpinning this article is why the EU engages with third countries on cyber issues, and through which channels. The main argument advanced 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. 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 positions EU cyber partnerships at the juncture between the emergence of the EU as a global actor and its attempts to develop so-called 'strategic partnerships' with other global powers, on the one hand, and the EU's increasing cyber actorness, on the other hand. The article then assesses these partnerships following an analytical framework based on three levels of expected purposes of these partnerships. Eventually, the article draws some broader reflections on the EU's cyber-diplomacy.

2. Framing the EU's cyber partnerships

Cyber partnerships are not unique to the EU. With the growing digitalization of our economies and societies, cyber issues have become a central item on the international agenda. All countries now interact and negotiate at various levels (bilateral, regional, global) to regulate this relatively new policy area, which is highly contested and still largely under-regulated (Segal, 2016). These 'cyber international relations' have broadened in scope and thickened in substance for a number of years already, and many partnerships have emerged in this context between allies and like-minded countries (such as between the US and Japan, for instance), but also between major cyber powers (such as China and Russia, for instance).

There is no definition of 'cyber partnership', a term I use essentially in reference to the broader EU 'strategic partnerships', as it will be further explained below. By way of definition, we could say that cyber partnerships are a form of cooperation between two international actors on cyber-related issues, based on shared interests and objectives, and underpinned by mutually agreed norms and mechanisms. As such, they are an advanced form of 'cyber international relations' beyond mere interactions, with the inclusion of a strategic and diplomatic dimension.

The EU's cyber partnerships came about as a result of two main developments: the EU's ambition to become a global strategic actor; and the incremental shaping of a European agenda on cyber issues. First, cyber partnerships would appear unnecessary, if not frivolous, had the EU not global normative ambitions. Indeed, the EU's international 'presence' and 'actorness' have significantly increased over the past decades, as referenced by several studies (Jupille and Caporaso, 1998; Bretherton and Vogler, 2006). This was the result of an extension of the EU's competences and capabilities, but also of the blurring between the 'internal' and 'external' agendas, which made the EU more of a global actor in spite of certain difficulties to shape a common foreign policy. The EU has also developed as a diplomatic actor, particularly in the post-Lisbon era, with increasing competences in key diplomatic functions such as representation, communication and negotiation – even registering significant diplomatic successes (Koops and Macaj, 2015; Smith, Keukeleire and Vanhoonacker, 2016).

Global and diplomatic actorness are of little use if they do not serve broader strategic objectives, however. As noted by Biscop and Andersson, 'without strategy any actor can really only be a "reactor" to events and developments' (Biscop and Andersson, 2008, p. 4). In fact, the Brussels institutions have been quite boulimic in their production of strategies, with the adoption of strategies for almost every issue and region of the world (Keukeleire and Delreux, 2014). The proliferation of such documents certainly indicate an intention to become more 'strategic', by identifying key objectives and priorities, even when the implementation of these strategies was not entirely convincing. The cybersecurity strategy adopted in 2013 can be partly seen in that context.

It is in this perspective of a more global, diplomatic-savvy and strategic Union that the EU developed a number of 'strategic partnerships' with global and emerging powers in the early 2000s. Of course, external factors influenced this development as well, notably a perceptible trend of power shift at the global level away from the transatlantic partnership, hence encouraging Europeans to rethink their diplomatic alignments. Partnerships, and particularly bilateral ones (as opposed to inter-regional ones), have become a key principle of the EU's

external action, as confirmed again in the 2016 EU Global Strategy (Renard, 2016; EEAS, 2016).

This development laid the foundation to the building of cyber partnerships, based on the EU's objectives and priorities in that area. However, that was only possible as the EU was becoming itself a cyber actor with global ambitions. The European institutions became involved in cyber-related issues already in the 1990s, but that involvement increased in the 2000s when the European Commission produced a number of communications, notably on Network and Information Security (2006) and on a Secure Information Society (2006). Even though the main focus of these initiatives was on the European level, the 'international' dimension was not entirely absent from the EU's concerns. In the 1990s already, the European Commission had 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 government 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).

More recently, the EU's cyber agenda has broadened considerably to embrace more systematically the international dimension of cyber issues, notably illustrated by the 2013 cybersecurity strategy, which included international priorities, and even more visibly with the adoption on European Council conclusions on 'cyber-diplomacy' in December 2015, which mark the beginning of a more proactive role of the EU in international cyberspace policy-making. The combination of the EU's global diplomatic and strategic footprint, resulting in the pursuit of 'strategic partnerships', with its broadening cyber agenda has paved the way for new cyber partnerships. Indeed, in both the 2013 strategy and in the 2015 conclusions, the Union is consistent with its broader strategic approach, based on 'partnerships' and 'multilateralism'.

In order to assess the functioning and purposes of these cyber partnerships, we turn towards the evaluation framework of EU strategic partnerships, developed by Grevi (2012) as well as Smith, Keukeleire and Vanhoonacker (2016), which identify three levels of 'purposes': 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, 2016).

Looking at cyber partnerships through the lens of strategic partnerships create a number of constraints. First, it limits the list of partners to the EU’s ten strategic partners (Brazil, Canada, China, India, Japan, Mexico, Russia, South Africa, South Korea and the USA), whereas the list of partners in the cyberspace may exclude some of these countries and include some others (such as Israel, for instance). Furthermore, strategic partnerships have been contested as a foreign policy instrument, particularly given the evolution of the EU-Russia strategic partnership in the aftermath of the crises in Ukraine and Syria. However, the evaluation framework presented here offers a key advantage: it has been used convincingly in previous studies (Smith, Keukeleire and Vanhoonacker 2016), and is sufficiently flexible to be applied in thematic policy areas. In this sense, evaluating strategic partnerships in the cyber domain is just one way of evaluating EU cyber partnerships, possibly paving the way for other similar studies. Furthermore, it is indeed useful to assess how strategic partnerships are being pursued and implemented across policy areas.

3. The reflexive level

With the growing importance of the internet in our economies and societies, but also with the correlate risks associated with cyber-crime and cyber-security, cyber issues have gained increasing traction on the international agenda over the past two decades. Some countries have asserted their strategic centrality in the new, ‘hacked’ world order (Segal 2016). That is notably the case of the traditional great powers, namely the US, China and Russia, but also of other ‘emerging’ or ‘middle’ powers, such as Brazil or South Korea, either due to their diplomatic strategies or to their technological edge.

In this hacked world order, there is no free seating. Cyber powers – or in other words, powers that have the ability to shape ‘the experience of those who act in or through cyberspace’ at the regional and global levels – must earn their place around the table, by right or might (Betz and Stevens, 2011, p. 44). In the case of Europe, it is clear that big EU member states like the UK, France and Germany belong to the group of cyber powers, in view of their civilian and military cyber capabilities. It is far less clear, however, whether the EU as an organisation can be considered as a cyber power.

To a large extent, the EU is a regional cyber power, as the EU institutions are certainly shaping European regulations, notably through the recent NIS Directive (on network and information security systems), which will strengthen the EU's member states cyber resilience, or via the capacity-building efforts of ENISA (the European Network and Information Security Agency). The global scope – geographically, but also thematically for that matter – of the EU's cyber power may be more debatable, due notably to issues of capabilities, competence or cohesion. Not being a state, the EU does not have the traditional instruments of 'hard power', such as military cyber capabilities even though it is now developing an embryonic cyber defence policy. But just like in many other policy areas, the EU aims to assert itself in the global arena through 'soft power' assets and diplomatic skills.⁴

In its 2013 cybersecurity strategy, the EU set a number of objectives that have far-reaching implications, including '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' (European Commission and High Representative, 2013). 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. The 2015 European Council conclusions on cyber-diplomacy went a step further by identifying specific foreign policy objectives, namely: 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).

Even though the EU had interacted with a number of international stakeholders before, the cybersecurity strategy and the Council conclusions on cyber-diplomacy gave a new meaning and dimension to the EU strategic partnerships in the cyberspace. The EU wanted to weight in international debates, and cyber-partnerships were perceived as a tool to do so. As European Commissioner Malmström had recognized before, it is fundamental for the EU 'to reach out to its strategic partners to make our response more effective' (Malmström, 2012). As a result, cyber issues were progressively added to the broader cooperation agenda between the EU and its strategic partners, making their way to the highest level of discussion as for instance 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.⁵ The EU has also largely formalised its partnerships, by establishing regular policy dialogues on cyber issues with all its partners (see below) and by adding a cyber chapter to the joint

⁴ On the importance of hard and soft power in cyberspace, see J. Nye, *The future of power* (PublicAffairs, 2011).

⁵ There was, for instance, a full section on cyber issues in the G7 Foreign Ministers Meeting in Lübeck, Germany, 15 April 2015.

cooperation agenda, when there is one (such as the EU-China 2020 Strategic Agenda for Cooperation).

As such the cyber-partnerships appear to perform a ‘positional’ function, in the sense that the Union has managed to assert itself as a worthwhile interlocutor in the cyber domain with all its strategic partners – and many more stakeholders – embedding them in a network of dialogues, joint statements and common initiatives, in which the EU becomes a hub, among many others indeed, but a significant player nonetheless with which other cyber power are willing to spend time and resources to engage at the technical, diplomatic and summit levels. In short, major cyber powers seem to consider that the EU has an added value in cyberspace policy, otherwise why would they engage at all?

The ‘positional’ function of cyber-partnerships is largely related to the ‘integrative’ one, however. 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 partner at the international level. ‘Integrative’ should not be understood in a narrow sense here, i.e. a transfer of competence to the EU institutions, but rather as the development of a more ‘integral’ or ‘comprehensive’ cyber policy – thus introducing more coherence between the different dimensions of the European cyber policy – and a more ‘integrated’ one – thus improving coordination between the EU and the national cyber policies, particularly vis-à-vis key partners.

Key cyber powers have consistently presented a major challenge to the EU’s overall cybersecurity and digital agenda, notably the US, Russia and China. The revelations of Edward Snowden, a former consultant for the US National Security Agency (NSA), about a US massive snooping programme have somewhat undermined the trust between the transatlantic partners. Espionage is nothing new, even among friendly countries, and Europeans reacted less strongly to that aspect than to the scope of the programme and to the risks of an excessive reliance on US-dominated internet and technologies. These revelations led to a shifting of views on cybersecurity, data protection and data privacy (Wright and Kreissl, 2013; West, 2014).

Cyber-espionage, for strategic or economic purposes, and cyber-attacks from Russia and China against European institutions and nations, confirmed or suspected, have been a major driver for a stronger European policy on cybersecurity and cyber-defence. Disagreements about cyber norms and the future of internet governance have also increased the need for a clear and coordinated position in this area, as expressed in the European Council conclusions stating that further development and implementation of a common and comprehensive EU approach for cyber diplomacy at the global level is ‘essential and crucial’. Indeed, 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’.

In sum, The multiple acts of cyber-espionage and cyber-offences from major powers 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. Overall, the EU's cyber-partnerships create a certain looping effect. Some partners challenge the EU in the cyberspace, hence requiring a stronger European response in terms of capabilities and coordination which in turn increases the significance and legitimacy of the EU as a global partner for these cyber powers.

4. Relational level

At the relational level, 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 the early 2000s, notably with the EC-US Task Force on Critical Infrastructure Protection, established in 2000. Today, the partnership relies primarily on the Working Group on Cyber-security and Cyber-crime (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).⁶ 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.⁷ 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.⁸ 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.

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

⁶ 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>

⁷ Interview with an EEAS official, Brussels, 16 April 2013; interview by email with an official from the EC3, 8 April 2013.

⁸ Interview 16 April 2013, op. cit.

Please note that there are some minor differences with the final published manuscript.

the broader transatlantic framework as a complement to the EU-US partnership.⁹ Cooperation also takes place on cyber-crime with Japan, notably 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 with Russia and 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, as well as of the track 1.5 Sino-European cyber dialogue. 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.¹⁰ 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.¹¹ 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.

Table 1: EU cyber dialogues with strategic partners

Partner country	Relevant dialogues
Brazil	Dialogue on international cyber policy; Information society dialogue
Canada	EU-US-Canada Expert Meeting on Critical Infrastructure Protection
China	Cyber taskforce; Dialogue on IT, telecommunications and informatisation
India	Political dialogue on cyber-security; Information society dialogue
Japan	Cyber dialogue; Dialogue on ICT policy
Mexico	Working Group on telecommunications; Dialogue on public security and law enforcement
Russia	Information society dialogue

⁹ Interview with an official from DG Home, Brussels, 13 May 2013.

¹⁰ Interview 8 April 2013, op. cit.

¹¹ Interview 16 April 2013, op. cit.

South Africa	Information society dialogue
South Korea	Cyber dialogue; Information society dialogue
USA	Working Group on Cyber-security and Cyber-crime (WGCC); Cyber dialogue; Information society dialogue; EU-US-Canada Expert Meeting on Critical Infrastructure Protection

Source: author own collection

In addition to joint initiatives and policy dialogues, cyber partnerships can be facilitated by legal acts, related to cooperation on criminal justice or law-enforcement, and by 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-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. 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.

In short, 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.

5. Structural level

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. The need for multilateral cooperation is enshrined in the EU’s Cyber-security Strategy, and 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 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.¹²

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

¹² Interview 16 April 2013, op. cit.

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 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.

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,

Please note that there are some minor differences with the final published manuscript.

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 bilateral 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.

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). 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.

5. EU cyber partnerships as a form of cyber-diplomacy

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 until recently. 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. 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.

Cyber issues are still not the most visible part of the EU’s global diplomatic efforts, however. 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.

At first sight, the EU cyber 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. After all, the EU cybersecurity strategy recommended to focus on ‘like-minded’ partners, thus acknowledging the inherent limits of ‘partnerships’ with China or Russia. 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,

Please note that there are some minor differences with the final published manuscript.

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. 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.

As way of conclusion, this article puts forward the concept of 'cyber-diplomacy', which has been advanced on several occasion through this article, and in EU documents, but without ever being properly defined or conceptualized. Possibly, EU cyber partnerships could be seen as a new form of diplomacy, or rather as a form of traditional diplomacy applied to a new policy area. In this regard, it would be necessary for more studies to look into this new concept, in order to better understand the meaning and functioning of cyber-diplomacy and, as a result, of EU cyber partnerships.

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.

Betz D. and T. Stevens, (2011) *Cyberpower and the State: Toward a Strategy for Cyber Power*, London: Routledge.

Biscop, S. and JJ. Andersson (eds), (2008) 'Introduction', in S. Biscop and JJ. Andersson, *The EU and the European Security Strategy: Forging a global Europe*, Abingdon: Routledge.

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.

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

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

Accepted Manuscript (AM) version.

Please note that there are some minor differences with the final published manuscript.

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

EEAS, (2016), *Shared vision, common action: A stronger Europe. A global strategy for the European Union's foreign and security policy*, Brussels: EEAS, June.

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-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.

Please note that there are some minor differences with the final published manuscript.

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).

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

Jupille, J. and J.A. Caporaso, (1998), 'States, Agency and Rules: the European Union in Global Environmental Politics', in: Rhodes, Carolyn (ed.), *The European Union in the World Community*, Boulder, CO: Lynne Rienner, pp. 213-229.

Keukeleire, S. and T. Delreux, (2014), *The Foreign Policy of the European Union*, London: Palgrave MacMillan.

Kleinwächter, W. (2008) 'Multi-stakeholder internet governance: the role of governments', in W. Benedek, V. Bauer and M.C. Kettman (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.

Koops, J. and G. Macaj (eds). (2015), *The European Union as a Diplomatic Actor*, London: Palgrave MacMillan.

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.

Please note that there are some minor differences with the final published manuscript.

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

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. (2016) 'Partnerships for effective multilateralism? Assessing the compatibility between EU bilateralism, (inter-)regionalism and multilateralism', *Cambridge Review of International Affairs*, 29(1), pp. 18-35.

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

Segal, A. (2016), *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, New York: PublicAffairs.

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.

West, S. (2014). 'Globalizing Internet Governance: Negotiating Cyberspace Agreements in the Post-Snowden Era', Conference Paper, TPRC 42: The 42nd Research Conference on Communication, Information and Internet Policy.

Wright, D. and R. Kreissl (2013), 'European responses to the Snowden revelations: A discussion paper', IRISS Working Paper (FP7), December.