ESP
EUROPEAN STRATEGIC PARTNERSHIPS OBSERVATORY

WORKING PAPER 7 | JUNE 2014

FRIDE
A EUROPEAN THINK TANK FOR GLOBAL ACTION

EGMONT

The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security

THOMAS RENARD

About ESPO. The purpose of the European Strategic Partnerships Observatory (ESPO) is to monitor the evolution and output of EU strategic partnerships – an increasingly important dimension of EU external action. It provides a unique source of data, analysis and debate on the EU's relations with a selected range of key global and regional players across different policy domains. ESPO's approach builds on two pillars, namely a focus on the state of bilateral partnerships and on the connection between partnerships and global issues. Through targeted work packages, ESPO aims to engage a wide network of experts and practitioners in Europe and beyond. ESPO is a joint initiative of FRIDE and the Egmont Institute. The ESPO website (www.strategicpartnerships.eu) is kindly supported by the Federal Foreign Office of Germany.

About FRIDE. FRIDE is an independent think-tank based in Madrid, focused on issues related to democracy and human rights; peace and security; and humanitarian action and development. FRIDE attempts to influence policy-making and inform public opinion, through its research in these areas.

About EGMONT. Egmont – Royal Institute for International Relations is an independent think tank, based in Brussels. Its research is organised along three main pillars: European affairs, Europe in the world, and African studies. The Egmont Institute was established in 1947 by eminent Belgian personalities.

THOMAS RENARD is a senior research fellow at Egmont – Royal Institute for International Relations, a Brussels-based think tank, and ESPO project leader at Egmont.

The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security

Thomas Renard

EU STRATEGIC PARTNERSHIPS AND TRANSNATIONAL THREATS

The purpose of the series of publications on 'EU strategic partnerships and international threats' is to provide evidence of the extent and limits of cooperation between the EU and its strategic partners on security issues, with a focus on transnational threats, namely nuclear non-proliferation, international terrorism, organised crime and cyber security.

This series includes four papers. It constitutes an original contribution to the existing literature on the subject, as it locates itself at the intersection between two distinct strands of research. On the one hand, there is a great amount of publications regarding these security issues and the EU's role in addressing them. On the other hand, there is growing literature on the EU's strategic partnerships, at a rather general level. This series will look into the operationalisation and implementation of all these partnerships in specific policy areas, including security. This crucial intersection offers a new and original angle to look at the EU's foreign policy, and to assess its effectiveness.

Already published in this series:

'Partnering for a nuclear-safe world: the EU, its strategic partners and nuclear proliferation' (October 2013).

'Confidential partnerships? The EU, its strategic partners and international terrorism' (January 2014).

'Partners in crime? The EU, its strategic partners and international organised crime' (May 2014).

C/ Felipe IV 9, 1º derecha. 28014-Madrid, España
T: +34 915 224 013
www.fride.org

All FRIDE publications are available at the FRIDE website: www.fride.org
All ESPO publications are also available at the ESPO website: www.strategicpartnerships.eu

ISSN 2254-6391 (print)
ISSN: 2254-6162 (Online)
Legal Deposit: M-23220-2012

Table of Contents

Cyber-security can no longer be disregarded by policy-makers. Governments worldwide have come to realise that their national security also depends on the security of their computers and technological devices. The European Union (EU) is no exception. Europe and the Brussels institutions are indeed a prime target for cyber-spies, cyber-attacks and cyber-crime. Over the past few years, Europe has stepped up efforts to reinforce its cyber-security, which were further encouraged by the unveiling of the US's large-scale surveillance programme, notably in Europe. Last December, the European Council urged the EU to strengthen its cyber-defence capabilities. This was a timely decision in view of the worsening situation in Ukraine and the consequent rise of cyber-attacks, including against European targets.

The EU has managed to raise significantly its profile on cyber issues, both domestically and globally. It is now a reliable interlocutor on cyber-crime and internet governance-related questions. Yet, it still needs to do more to become a global 'cyber power'. This paper focuses on the EU's global role in cyber-security, and its cooperation with its strategic partners.

Assessing the threat

Among the so-called non-traditional security issues, cyber-security is probably the one that has gained most prominence in recent years. Whereas twenty years ago very few considered cyber-security a challenge, today it is seen as one of the greatest challenges to international security. This is due, among other factors, to society's increasing reliance on the internet and on information and communication technologies (ICTs), as well as to the growing sophistication of cyber-attacks.

Most of our critical infrastructures (electricity grids, the banking system, transportation, etc) rely in part or entirely on the internet and ICTs. Recent research also suggests that our economies increasingly depend on these technologies, which account on average for 3.4 per cent of GDP in developed countries and 21 per cent of global GDP growth in 2004–9.[1] Growth related to the 'internet economy' is estimated to be at 11 per cent in the EU, with a share of European GDP expected to rise from 3.8 per cent in 2010 to 5.7 per cent in 2016, according to the Boston Consulting Group.[2]

The growing sophistication of cyber-attacks has attracted equal attention in recent years. The Stuxnet virus, discovered in 2010, is a good example. The virus targeted a specific

[1] McKinsey, 'Internet matters: the Net's sweeping impact on growth, jobs and prosperity', McKinsey Global Institute, May 2011.
[2] D. Dean et. al., 'The internet economy in the G-20: The $4.2 trillion growth opportunity', Boston Consulting Group Report, 2012.

piece of IT equipment of Iran's nuclear facilities with the objective of slowing down Tehran's nuclear programme. This was a highly intricate manoeuvre, allegedly developed by the US and Israel.[3] Every day, countless attacks, including extremely sophisticated ones, are launched by both governments and non-state actors. The scope of activities is very broad and could have direct implications for 'real' security, such as 'trigger[ing] a meltdown in a functioning nuclear power plant, turn[ing] off oil and gas pipelines or chang[ing] the chemical composition of tap water'.[4] In fact, what seems to be melting or fading away is the border between virtual and real security.

Cyber-security is a complex reality with many dimensions. Responding to the cyber challenge requires a good understanding of this complex issue. Following Joseph Nye, this document identifies four different categories of cyber-attacks, which together make up the pillars of cyber-insecurity.[5]

(1) Cyber-crime: cyber-criminality, similar to 'regular' criminality, includes a vast range of activities, such as petty theft, massive financial fraud, child pornography, etc. Cyber-criminality is the most visible of all cyber-threats, and also the most widespread In general, cyber-criminals mainly seek to make a profit, which distinguishes this type of activities from politically-motivated cyber-attacks. Although it is very difficult to measure the scope of this business, it is deemed to be expanding and quite lucrative. It is estimated that it costs the economy several billion US dollars each year, with some studies, such as a report from Norton, claiming costs of hundreds of billions, up to US$ 388 billion annually.[6]

(2) Cyber-espionage: cyber capacities can be used for traditional or industrial espionage. In recent years several allegations and leaks, including by the American consultant Edward Snowden, have shown that various governments worldwide collect data and intelligence on citizens, companies and governments in the cyber-space. One example was GhostNet, a virus discovered in 2009, which targeted thousands of computers from various foreign ministries, embassies, news agencies and NGOs worldwide to steal possibly-sensitive information. More recently, the US pressed legal charges against five members of the Chinese PLA Unit 61398, following suspicions of extensive breaches into US government and corporate targets since 2006.[7]

(3) Cyber-terrorism: terrorist groups have been active on the internet for some time, with the aim of radicalising and recruiting new members. The internet can also be used for financing purposes, as well as for planning attacks, for instance through the use of intelligent services such as Google Earth. Terrorist groups could also launch full-scale cyber-attacks to pursue their political objectives. Some security experts believe that there is a credible risk of cyber-attacks from terrorist groups in the future.

(4) Cyber-warfare between states: although the likelihood of a 'pure' form of cyber-warfare is debatable,[8] the cyber-space increasingly ends up becoming an integral part of diplomatic or military conflicts. In the current Ukrainian crisis, cyber-attacks have been carried out against Ukraine (including its military communications system), Russia, European countries, and NATO. Allegedly, Russia was even able to take control of an American drone in Crimea.[9]

[3] V. Manzo, 'Stuxnet and the dangers of cyberwar', *The National Interest*, 29 January 2013.

[4] World Economic Forum, 'Global risks 2012', Seventh edition, *Insight Report*, 2012, p. 25.

[5] J. Nye, *The future of power* (New York: PublicAffairs, 2011).

[6] Symantec, 'Norton study calculates cost of global cybercrime: $114 billion annually', *Press Release*, 7 September 2011. For an account of various studies, see N. Robinson et. al., 'Feasibility Study for a European Cybercrime Centre', *Technical Report*, RAND Corporation, 2012, pp. 31-55.

[7] M.S. Schmidt and D.E. Sanger, '5 in China Army Face U.S. Charges of Cyberattacks', *New York Times*, 19 May 2014.

[8] T. Rid, *Cyber war will not take place* (New York: Oxford University Press, 2013).

[9] Defense update, 'The Ukrainian crisis – a cyber warfare battlefield', *Defense update*, 5 April 2014. Available online at: http://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html#.U0KecCjN822

All of this indicates that cyber-security is not an entirely new challenge. Rather, it brings a new dimension to existing challenges (criminality, espionage, terrorism/political violence and war). While the instrument is new, the *finalité* remains unchanged. In confronting this challenge there is no need to reinvent the wheel, but rather to adapt existing tools and develop new ones, mostly within existing structures, to deal with the technical specificities of the virtual world.

Europe has been a prime target of cyber-attacks across the four categories. Many cyber-incidents have been reported in recent years, with a trend pointing to an increase in terms of both frequency and sophistication of the threat.[10] As a major connected economy, Europe is a fertile ground for cyber-criminality, which reportedly already costs the UK alone €30 billion a year.[11] The EU institutions themselves have been a target of cyber-attacks. In 2011, a breach of 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.[12] European governments and companies are also extensively exposed to cyber-espionage, notably from Russia and China, but also from the US.[13] With regard to cyber-terrorism, Europe has seen a growing number of 'lone-wolf' terrorists in recent years, self-radicalised through the internet. Europol also pays close attention to the risk of cyber-attacks by terrorist groups. It discussed this specific threat for the first time in its 2012 annual threat assessment.[14] In 2007, Estonian servers were also victims of cyber-attacks, generally attributed to Russia, awakening Europe to the reality of 'cyber-warfare'.[15] On the basis of the growing cyber threat, Europe has attempted to develop a more strategic approach and to strengthen cyber-security capabilities at the national, regional (EU and NATO) and global levels (G8, UN, etc.).

EU citizens are also concerned with their cyber-security. According to a 2011 poll, 81 per cent of EU citizens believe that cyber-crime is an important challenge to the EU's internal security, although not necessarily the most pressing one.[16] They also believe that the cyber challenge in general is becoming more important. According to a 2013 poll, 76 per cent of EU citizens believe that they are more exposed to cyber-criminality now than they were before.[17] As a result, many Europeans would like to see a more pro-active EU in the area of cyber-security. Among all security challenges, this is the one where the most EU citizens (36 per cent) consider that the EU could do more.[18] There is therefore popular support for an EU-wide response to cyber-security.

The EU's strategic approach

European concerns over cyber-security date far back, but have been compounded in recent years by two factors in particular. On the one hand, the increase in cyber-criminality and cyber-attacks has underscored Europe's vulnerability to these kinds of threats. On the other hand, the persistence of

[10] Robinson 2012, op. cit. See also Europol, *Threat assessment: Internet facilitated organised crime (iOCTA)* (The Hague: Europol, January 2011).

[11] Detica, 'The cost of cyber crime', *Detica Report*, February 2011.

[12] House of Lords, 'The EU internal security strategy', *Report*, 17th Report of Session 2010–12, May 2011, p. 39.

[13] P. Apps and J. Finkle, 'Suspected Russian spyware Turla targets Europe, United States', *Reuters*, 7 March 2014; FireEye, 'FireEye Uncovers Chinese Cyber Espionage Campaign Targeting European Ministries of Foreign Affairs', *Press Release*, 11 December 2013. Available online at: http://investors.fireeye.com/releasedetail.cfm?ReleaseID=813251

[14] Europol, *TE-SAT 2012* (The Hague: Europol, 2012).

[15] See e.g. S. Herzog, 'Revisiting the Estonian cyber attacks: digital threats and multinational responses', *Journal of Strategic Security*, 4:2, 2011, pp. 49-60.

[16] European Commission, 'Internal security', *Eurobarometer 371*, November 2011.

[17] European Commission, 'Cyber security', *Eurobarometer 404*, November 2013.

[18] European Commission, 'Internal security', November 2011, op. cit.

the economic crisis and the hunt for growth has underlined the need for cyber 'trust and security', as acknowledged in the Digital Agenda for Europe.[19]

The EU is not short on 'strategies' to deal with cyber-challenges. In 2001, the European Commission had already published a communication entitled 'Network and Information Security: proposal for a European Policy approach',[20] which identified key challenges and formulated some recommendations regarding the issue. This was reinforced in 2006 by the communication on 'A Strategy for a Secure Information Society', which advocated a European information society based on a growing culture of security.[21] Several other communications followed, always highlighting concrete challenges in specific dimensions of cyber-security, such as cyber-crime or the protection of critical information infrastructures (CIIP), defined as 'those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy'.[22] With regard to cyber-terrorism, the 2005 counter-radicalisation strategy made clear references to the importance of the web.[23] Cyber-security is now explored in the six-monthly progress reports of the EU's counter-terrorism coordinator.

These developments notwithstanding, until the end of the last decade the EU had approached the issue of cyber-security 'in a fragmented manner, where parallel policies have been launched with different overlapping themes'.[24] In 2008, however, cyber-security was identified as a key challenge in the review of the European Security Strategy (ESS) and, two years later, in the Internal Security Strategy (ISS). A more strategic approach was mandated. The ISS made a first contribution by identifying three clear objectives: building capacities in law enforcement and judiciary, working with industry, and improving capabilities for dealing with cyber-attacks. This was complemented by a Cyber-crime Action Plan adopted by the European Council in 2010.[25]

In February 2013, the EU adopted its long-awaited Cyber-security Strategy.[26] As it was a joint initiative by the Commission and the High Representative, it was able to bridge the different facets of the cyber-challenge into a single document, i.e. internal security (including cybercrime and CIIP), external security, and foreign and defence policies. The document is articulated around five strategic priorities:

[19] European Commission, 'A digital agenda for Europe', *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM(2010)245 final, 2010. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:HTML

[20] European Commission, 'Network and Information Security: proposal for a European Policy approach', *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM(2001)298, 2001.

[21] European Commission, 'A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"', *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM(2006)251, 2006. Available online at: http://ec.europa.eu/information_society/doc/com2006251.pdf

[22] European Commission, 'Towards a general policy on the fight against cyber crime', *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,* COM(2007)267, 2007. Available online at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52007DC0267; European Commission, 'Achievements and next steps: towards global cyber-security', *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM(2011)163, 2011. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

[23] Council of the EU, 'The European Union strategy for combating radicalisation and recruitment to terrorism', *14781/1/05*, 2005. Available online at: http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2014781%202005%20REV%201

[24] A. Klimburg and H. Tirmaa-Klaar, 'Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU', *European Parliament Study*, April 2011, p. 29.

[25] Council of the EU, 'Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime', 3010th General Affairs Council meeting, Luxembourg, April 2010. Available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611cccybercrime_/sede150611cccybercrime_en.pdf

[26] European Commission and High Representative, '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*, JOIN(2013)1, 2013. Available online at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

- Achieving cyber resilience, which includes member states developing their national capabilities (to avoid the 'weak link' problem) as well as a 'cyber-security culture'
- Drastically reducing cyber-crime, which includes the need for 'strong and effective legislation', as well as improved coordination at EU level
- Developing cyber-defence policy and capacity related to the Common Security and Defence Policy (CSDP), which includes a call for better cooperation between the EU and NATO
- Developing industrial and technological resources for cyber-security
- Establishing a coherent international cyber-space policy for the EU and promoting core EU values, which include the need to deepen dialogue with third countries 'with a special focus on like-minded partners that share EU values' and international organisations, as well as stepping up capacity-building programmes in third countries, sometimes in cooperation with other stakeholders.

While this more integrated approach represents a step forward in dealing with one of the most serious global challenges of our time, the EU is lagging well behind the US in this regard, not least because its member states are themselves lagging behind. In 2003 Washington adopted a cyber-strategy, while only a few EU member states have one today. The EU should thus encourage its member states to invest more in their cyber-security, with a view to turning Europe into a real cyber force. In terms of budget, the EU is investing significant amounts in this area, with over €500 million foreseen under the research and innovation programme 'Horizon 2020'.[27] Several projects have also been funded under DG Home's ISEC (now IFS Police) financial instrument.[28] However, most of this money is to be spent domestically. In its external relations, the EU had budgeted a meagre €15 million under its Instrument for Stability (IfS) for 2012-13 to cope with organised crime, of which a small fraction was dedicated to cyber-crime. While funding is still very marginal, it can be seen as the beginning of the EU's international role in cyber-security (no funding was foreseen for this area under this instrument prior to 2012).

According to Neelie Kroes, the EU Digital Agenda commissioner, the EU's cyber-security depends on its ability to coordinate across sectoral policies, not solely in member states but also in cooperation with key international stakeholders. A common European approach would allow the EU to become a more strategic and trusted partner at the international level, with positive benefits for its security and competitiveness.[29] The EU has been active in defining a 'global coordination strategy' and a 'shared framework' to make the internet safe and stable.[30] Similar to other challenges, in cyber-security the EU has developed a flexible multi-layered approach, engaging with a variety of stakeholders at the multilateral, regional and bilateral levels.

The EU's cyber-security strategy recommends working with international partners and organisations. Among the multilateral organisations included is the United Nations. The UN General Assembly adopted a number of resolutions related to cyber-security, contributing to raise global awareness about this issue. The UN Counter-terrorism Committee has also been active, along with the UN Disarmament Committee, which produced an important report on cyber-security in 2010.[31] Two

[27] European Commission, 'Horizon 2020: Work programme 2014-2015. Part 14', *Decision C (2013)8631*, 10 December 2013. Available online at: http://www.statewatch.org/news/2013/dec/com-2013-horizon-2020-security-wp.pdf

[28] European Commission, 'Table on the Implementation of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"', *Working document*, 28 February 2014. Available online at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4623

[29] N. Kroes, 'Towards a coherent international cyberspace policy for the EU', *Speech at the Global Cyber Security Conference*, Brussels, 30 January 2013. Available online at: http://europa.eu/rapid/press-release_SPEECH-13-82_en.htm?locale=en

[30] European Commission, 'Achievements and next steps: towards global cyber-security', 2011, op. cit.

[31] UNGA, 'Report of UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', *A/65/94*, 24 June 2010.

organisations are particularly relevant with regard to internet governance, although to a certain extent with competing approaches: one based on a government hands-off approach and the other on a more traditional form of international governance. The Internet Corporation for Assigned Names and Numbers (ICANN), the world's most important web regulator, illustrates the first model. Despite being a non-governmental organisation, ICANN has an active Government Advisory Council. The US is particularly influential in this forum, where the EU is also represented. The International Telecommunications Union (ITU), a UN-agency, illustrates the second model. It has played a key role in many UN initiatives in the cyber-space. Other relevant organisations include the Organisation of Economic Cooperation and Development's (OECD) Working Party on Information Security and Privacy (WPISP), which develops policy recommendations on the information society and resilience building, as well as the G8, which has established a sub-group on high-tech crimes.

The Council of Europe's 2001 Convention on Cyber-crime, known as the Budapest Convention, is the cornerstone of international cooperation on cyber-crime.[32] The convention is significant because its signatories are legally bound by common standards and procedures, and it facilitates operational cooperation. It is the sole example of this kind of international cyber-security agreement. It was signed by 49 countries and ratified by 42, including countries that are not part of the Council of Europe. Promoting this convention worldwide is one of the EU's objectives .[33]

At the regional level, the cyber-security strategy highlights some organisations with which the EU should seek 'closer cooperation'. In a broader European context, it argues that the EU should work more closely with NATO, which has developed several instruments to cope with cyber-security, and more specifically with cyber-defence. The Organisation for Security and Cooperation in Europe (OSCE) is also mentioned. Beyond Europe, the strategy envisages that the EU could also cooperate with other regional organisations, such as the African Union (AU), the Association of Southeast Asian Nations (ASEAN) or the Organisation of American States (OAS).

Finally, the EU's international cyber efforts rely on strategic partnerships with third countries. The importance of bilateral dialogues was already mentioned in previous European Commission documents, emphasising the need for 'strategic cooperation with third countries' to reach a global consensus on internet resilience and stability,[34] or calling for 'a global coordination strategy reaching out to key partners'.[35] The 2013 Cyber-security Strategy recommends placing a 'renewed emphasis on dialogue with third countries'. Although the EU has ten strategic partners,[36] alike in previous EU documents the US is singled out. According to the strategy, the transatlantic partnership is 'particularly important and will be further developed'. With regard to other potential partners, the EU should have a 'special focus on like-minded partners that share EU values'. Cooperation with some strategic partners, such as Russia or China, is thus implicitly dismissed.

The 2013 Cyber-security Strategy also presents the objectives of such partnerships. These include the exchange of information and best practices, the coordination of policies and of capacity-building efforts in third countries, the strengthening of multilateral instruments, and the promotion of sustainable internet governance.

[32] See: European Commission, 'Towards a general policy on the fight against cyber crime', 2007, op. cit.

[33] IHEDN, 'Towards a European cyberstrategy?', Conference Report, *4th IHEDN Brussels Day*, 28 June 2012.

[34] European Commission, '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*, COM(2009)149, 2009. Available online at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52009DC0149

[35] European Commission, 'Achievements and next steps: towards global cyber-security', 2011, op. cit.

[36] Brazil, Canada, China, India, Japan, Mexico, Russia, South Africa, South Korea and the United States.

The challenge of implementation

Although it is a global challenge in nature, and despite some steps at EU level, European cyber-security remains almost exclusively a national prerogative. The 2013 Cyber-security Strategy acknowledges that dealing with security challenges in the cyber-space is 'predominantly the task of member states'.[37] European capitals have taken some interesting initiatives in this area. France, the Netherlands and Germany have established government departments directly concerned with cyber-security. Since Estonia adopted the first cyber strategy in Europe (in 2008), 17 member states have drafted their own cyber-security strategies, including the UK, France, the Netherlands, the Czech Republic and Belgium (in 2013). There are 23 Computer Emergency Response Teams (CERTs) in Europe. Sometimes compared to fire-fighters, the CERTs are the main instrument to ensure CIIP and are the first to react in case of an information security incident. The budget and staff allocated to cyber-security vary greatly from one country to another.[38] The same is true for the level of preparedness and capability, although it is generally considered insufficient in most countries,[39] either due to weak capabilities or a lack of cooperation between the relevant communities, notably law-enforcement agencies (LEAs) and CERTs.[40] This constitutes a major problem since it is considered that weaker member states can undermine the collective security of the EU as a whole.[41]

As recognised by the member states themselves,[42] cyber-security must take place within a broader context, in which the EU can complement (rather than replace) and coordinate their actions. A major instrument for coordinating European activities is the Policy Cycle.[43] Based on Europol analysis, the EU and its member states have identified key cyber-crime priorities, which they pursue in joint cooperation through an operational action plan.[44] The Friends of the Presidency Group on Cyber Issues, a working group within the structures of the Council of the EU, is another key instrument. Launched in 2012, it provides a venue for member states to ensure horizontal coordination on cross-cutting cyber issues and to exploit potential synergies among them.

Cooperation and coordination between various national agencies is necessary, but at the same time quite challenging given the multitude of actors, who are not always used to working together and might lack the sufficient level of mutual trust to do so. For instance, an effective cyber response often requires collaboration between CERTs and LEAs, although these two security communities do not have natural cooperation reflexes. Cross-border investigations render this even more complicated. A recent report by ENISA pinpointed this problem and suggested some possible ways forward.[45]

ENISA provides expertise, advice and assessment of cyber-practices in Europe to European institutions and member states. It also facilitates dialogue among the various actors involved

[37] European Commission and High Representative, 2013, op. cit.

[38] Robinson 2012, op. cit., pp. 56-83.

[39] B. Grauman, 'Cyber-security: The vexed question of global rules', Security and Defence Agenda, 2011. See also ENISA, 'The fight against cybercrime: Cooperation between CERTs and law enforcement agencies in the fight against cybercrime', European Network and Information Security Agency (ENISA), 2012; Robinson 2012, op. cit.

[40] ENISA 2012, op. cit., p. 1.

[41] House of Lords 2011, op. cit., p. 47.

[42] See for example the UK cyber-security strategy 'Protecting and promoting the UK in a digital world', 2011.

[43] See the previous paper in this series: T. Renard, 'Partners in crime? The EU, its strategic partners and international organised crime', *ESPO Working Paper* 5, May 2014.

[44] European Commission, 'Table on the Implementation of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"', 2014, op. cit.

[45] ENISA 2012, op. cit.

in cyber-security at EU level. In 2010, it organised the first pan-European exercise for critical IT Infrastructure Protection (named Cyber Europe 2010), which highlighted the fact that there was no pan-European procedure to respond to a cyber-attack. A third exercise is planned for 2014, in cooperation with EU member states, EFTA countries and EU institutions. ENISA was established in 2004 and has seen its role gradually expand to become a major actor in the European cyber-security community. It employs approximately 65 personnel, and has an annual budget of approximately €8 million.[46]

Whereas ENISA works mostly with CERTs, Europol is connected to the intelligence and law-enforcement communities. Europol focuses essentially on cyber-crime. It supports member states in many ways in their investigations. Since 2010, the agency has produced its own Internet-Facilitated Organised Crime Threat Assessment (iOCTA).[47] Europol's role has grown since the inception of the Cyber-crime Centre (EC3) in 2013, located within its offices. It is set to become 'the focal point in fighting cyber-crime'.[48] It has a staff of around 50 people and an annual budget of around €10 million.[49] In the future, Europol and ENISA should cooperate more and more to bridge the existing gap between different cyber-security communities. In 2012 the two agencies held their first joint meeting.[50]

Other relevant actors include Eurojust, which plays a role in the fight against cyber-criminality by facilitating cooperation among prosecutors; the European Commission, which formulates strategies and policies, and more specifically DG Home (which overviews Europol's activities) and DG Infso (which overviews ENISA's activities); the CERT-EU established in 2011; and the EDA, which has defined cyber-defence as one of its 'Top 10 priorities'[51] and is in charge of further developing the EU's capabilities in this important area, together with the EU Military Staff (EUMS).

All of these EU cyber actors are mostly active within the EU, but some of them are also active externally. For instance, DG Infso plays a 'decisive role'[52] in the meetings of the EU-US Working Group on Cyber-security and Cyber-crime. And ENISA facilitated the planning of the first EU-US cyber-security exercise.[53] The EC3 also interacts directly with international counterparts. Within the EU's foreign policy structures (CFSP), however, few institutions deal with these issues. Until very recently there was only one person working on this issue within the European External Action Service (EEAS), and few more within the EDA. There are now four national cyber experts seconded to the EEAS, indicating a growing interest regarding this question.

On top of existing actors, new capabilities and organisations are being established in every member state, as well as at EU level. The challenge is in fact twofold: coping effectively with the cyber-challenge at all levels, while avoiding too deep a fragmentation of actors and competences, which would be counter-productive. In this regard, some experts have suggested the appointment of

[46] Robinson 2012, op. cit.

[47] Europol, *Threat assessment: Internet facilitated organised crime (iOCTA)*, January 2011, op. cit.

[48] European Commission, 'An EU Cybercrime Centre to fight online criminals and protect e-consumers', *Press Release*, 28 March 2012. Available online at: http://europa.eu/rapid/press-release_IP-12-317_en.htm

[49] EC3, *First year report*, The Hague: Europol, 9 February 2014.

[50] Enisa, 'First ENISA-EuroPol meeting taking place in Crete', *Press Release*, 30 January 2012. Available online at: http://www.enisa.europa.eu/media/news-items/first-enisa-europol-meeting-taking-place-in-crete

[51] See the EDA's website: https://www.eda.europa.eu/Aboutus/Whatwedo/capability-development-plan. We should note here that regarding cyber-defence in Europe, NATO also plays an important role.

[52] Klimburg and Tiirma-Klaar 2011, op. cit., p. 33.

[53] U. Helmbrecht, 'EU cyber security and the role of ENISA', in P. Hario and S. Heinikoski (eds), *The European Union as a security provider*, *Research Report 48*, National Defence University, 2011, pp. 49-66.

a cyber-security coordinator at EU level.[54] Overall, much effort is still needed for the EU to be considered a fully strategic player in this field.

As the EU tries to raise its global profile in cyber-security, it increasingly seeks cooperation and coordination with international actors, including its strategic partners. The architecture of strategic partnerships is thus being progressively adapted to integrate cyber issues. Discussions can take place at the highest level, between respective leaders. These issues occasionally appear in joint statements, but have not yet been a central theme of any summit. Such statements can be relatively lengthy and indicate a good level of cooperation or the launch of new initiatives, such as with Japan or the US, or they can be more succinct, suggesting insetad an intention to explore cooperation, such as with China, India or Brazil. With all the other partners, however, cyber-security has never been discussed or mentioned at summit level, reflecting the marginal though nascent importance of this issue in these partnerships.

Discussions of cyber-security can also take place at the ministerial level. For instance, cyber-crime has been tackled within the framework of the EU-US justice and home affairs ministerial meeting, which gathers twice a year. The issue has also been addressed in the past by the EU-Russia Permanent Partnership Council (PPC), although it has essentially disappeared from the agenda of recent meetings. 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. With all the EU's other partners, cyber-security has not been addressed at ministerial level.

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.'[55] 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. There is also a trilateral EU-US-Russia dialogue on justice and home affairs that was initiated in 2006 and which could address cyber issues,[56] although this dialogue is now dormant.

Other partnerships are significantly less developed. An EU-China Cyber Taskforce was established in 2012. The EU and India meet annually in the context of the political dialogue on cyber-security. 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 yet been the case. A number of ICT-related dialogues are in place with some partners, in the framework of which certain

[54] P. Cornish, 'Cyber security and politically, socially and religiously motivated cyber attacks', *European Parliament Study*, February 2009.

[55] EEAS, 'EU-US cooperation on cyber security and cyberspace', *Fact Sheet*, 26 March 2014. Available online at: http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf

[56] EU-Russia-USA, *Communiqué*, Meeting at Ministerial Level, 4 May 2006. Available online at: http://www.libertysecurity.org/IMG/pdf/draft_press-communique-MP_04_05_final.pdf

issues such as internet governance can be addressed. These include 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 the most recent EU-Mexico Working Group on telecommunications, announced in 2013.[57]

In addition to these dialogues, cyber-security issues can be addressed in the context of inter-parliamentary encounters. This has been the case between the EU and the US, for instance, within the framework of the transatlantic legislators dialogue.[58]

Partnering on cyber-security

The EU is developing a more strategic approach to cyber-security and is improving its cyber capabilities. Although it cannot yet be considered a global cyber power, and despite the fact that most activities are still undertaken at national level, the EU has emerged as a reliable international interlocutor on cyber issues. This section reviews the EU's cooperation with its strategic partners on cyber-security.

Exchange of information and best practices

Bilateral cooperation is essential to efforts to cope with the new cyber challenge. Strategic partnerships should therefore play a key role in shaping a more effective response to this global challenge, as emphasised by European Commissioner Cecilia Malmström.[59] Yet, the level for cooperation varies from among the EU's ten strategic partners.

The EU-US bilateral partnership is by far the most developed. It relies on the WGCC, which identifies clear priority areas for cooperation, as well as concrete deliverables, following a specific roadmap.[60] 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 CIIP (in 2010). The joint exercise brought together over 100 government experts from both sides to assess responses to cyber-espionage and cyber-attacks. Another fully-fledged exercise is foreseen in 2014.

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.[61] The US is also considered a key cooperation partner in science, technology and innovation in relation to cyber security.[62] The EU-US partnership is perhaps the only one sufficiently advanced to consider triangulated efforts for

[57] EU-Mexico, 'Joint Communiqué', *XII Joint Committee European Union-Mexico*, 10-11 June 2013. Available online at: http://eeas.europa.eu/delegations/mexico/documents/news/20130612com_xii_comite_conjunto_ue_mx_en.pdf

[58] EU-US, 'Joint statement', *73rd Interparliamentary meeting*, 1 December 2012. Available online at: http://eeas.europa.eu/us/docs/2012_tld_joint_statement_en.pdf

[59] C. Malmström, 'The European Response to the rising Cyber Threat', *Speech at the Transatlantic Cyber Conference*, Washington, 2 May 2012. Available online at: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/315

[60] EU-US, 'Concept Paper', *EU-US Working Group on Cyber-security and Cyber-crime*, 13 April 2011.

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

[62] European Commission, 'ICT research and innovation in a globalised world', ISTAG Working Group on International Cooperation, March 2012, p. 58.

cyber capacity-building in third countries. Discussions for a coordinated approach have been initiated.[63] There is thus a thick network connecting both partners, allowing for broad and effective cooperation.

Beyond the US, there are numerous contacts with Canada, mainly with regard to cyber-crime and CIIP. The partnership with Canada is usually seen within a broader transatlantic framework, and as a complement to the EU-US partnership, rather than as a stand-alone partnership.[64] Cooperation also takes place on cyber-crime with Japan, notably through the EC3. Other cyber-security issues, such as CIIP and smartphones security, have been discussed between ENISA and a Japanese agency.[65] 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'.[66] Besides, the EU and Japan have funded joint research projects on cyber-security.[67] Similarly, the EU and Brazil have unlocked joint funding under their research programmes to address 'internet governance and security'.[68]

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 even the discussions around the modalities of the taskforce were rather difficult, reflecting the deep rift between the two partners.[69] The EU also supports China in the development of data protection laws.[70] More cooperation is foreseen in the future, as expressed in the EU-China 2020 Strategic Agenda for Cooperation, notably on cyber-crime.[71] With Russia, cooperation first focussed on the use of the 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.[72] 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.[73] Overall, however, cooperation remains limited. The current Ukrainian crisis is exacerbating tensions between the two parties, although operational cooperation remains largely unaffected at this stage.

With the rest of the EU's 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.[74] The 2010 Framework Agreement with

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

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

[65] ENISA, 'ENISA hosting the Japanese Information-technology Promotion Agency, "IPA"', *Press Release*, 15 December 2011. Available online at: http://www.enisa.europa.eu/media/news-items/enisa-hosting-the-japanese-information-technology-promotion-agency-201cipa201d/view?searchterm=None

[66] MIC, 'Outcome of 19th Japan-EU ICT dialogue and Japan-EU Internet Security Forum', *MIC Communication News*, 28 November 2012.

[67] European Commission, 'EU-Japan ICT Cooperation – joining forces for the Future Internet', *Digital Agenda for Europe webpage* [Accessed on 7 May 2014]. Available online at: http://ec.europa.eu/digital-agenda/en/eu-japan-ict-cooperation-–-joining-forces-future-internet

[68] European Commission, 'Digital Agenda: EU and Brazil strengthen ties with '10 million joint ICT field research programme', *Press Release*, 8 November 2011. Available online at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1316

[69] Sénat de Belgique, 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

[70] P. Pawlak and C. Sheahan, 'The EU and its (cyber) partnerships', *Brief Issue* 9, EU Institute for Security Studies, March 2014.

[71] EU-China, 'EU-China 2020 Strategic Agenda for Cooperation', 21 November 2013. Available online at: http://eeas.europa.eu/china/docs/eu-china_2020_strategic_agenda_en.pdf

[72] Interview 8 April 2013, op. cit.

[73] R. Hernandez i Sagrera and O. Potemkina, 'Russia and the Common Space on Freedom, Security and Justice', *CEPS Paper in Liberty and Security in Europe* 54, February 2013.

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

South Korea proposed cooperation and consultations on cyber-crime, but this has taken time to materialise. 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[75]

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; 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 because 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 JHA international agreements signed by the EU. Japan is the only other strategic partner with whom the EU has signed an MLA agreement, in 2009. It should be noted that the EU-US agreements offer a framework for cooperation, but they nonetheless co-exist with bilateral agreements between the US and EU member states. The EU-Japan MLA agreement, on the other hand, is a self-standing accord, making up for the absence of bilateral agreements with EU member states. It thus offers significant added value. 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.[76] 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 expert meetings with Russia in Europol, and a decision was taken to establish a cyber-crime platform in Europol that would permanently include Russian experts.[77] In 2009, the Council of the EU mandated Europol to start negotiating an operational agreement with Russia to deepen cooperation, although the conclusion of this agreement remains difficult.[78] Joint workshops were organised on personal data protection to strengthen mutual trust. Agreements

[75] This section draws extensively from the same section in the previous paper of this series, focussing on organised crime. Many agreements on organised crime cover indeed cyber-crime as well.

[76] J. Monar, 'The external dimension of the EU's area of freedom, security and justice: Progress, potential and limitations after the Treaty of Lisbon', *Report* 1, Swedish Institute for European Policy Studies, 2012, p. 58.

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

[78] Council of the EU, '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

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. It is currently on hold due to political tensions. 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.[79] 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.[80] 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 only international instrument singled out.

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.[81] 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.[82]

The US and Japan have signed and ratified the convention. 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.[83] Canada and South Africa have 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 are being 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 Council of Europe until the end of

[79] Eurojust, *Annual Report 2009* (The Hague: Eurojust, 2010). Available online at: http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202009/Annual-Report-2009-EN.pdf

[80] Ibid.

[81] A. Bendiek, 'Tests of partnership: Transatlantic cooperation in cyber security, internet governance and data protection', *Research Paper 5*, Stiftung Wissenschaft und Politik, March 2014, p. 10.

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

[83] EU-US, 'Concept paper', 2011, op. cit.

2014 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 and they tend to coalesce with China and Russia over cyber-issues in multilateral fora.[84]

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. The UN and the ITU are two organisations where the EU has interacted with its partners. In the framework of the UNODC expert group on cyber-crime, the EU and the US regularly coordinate positions. The G8 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).[85] The so-called 'London Process' is yet another platform for discussing cyber issues. Initiated by UK Foreign Secretary William Hague in 2011, it convenes 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 framework of the NATO-Russia Council.

Shaping internet governance

The broader question of internet governance appears to be particularly contentious. 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'[86]:

[84] Interview 13 May 2013, op. cit.

[85] European Commission, 'Table on the Implementation of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"', 2014, op. cit.

[86] Klimburg and Tiirma-Klaar 2011, op. cit., 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.

Internet governance has become an increasingly divisive foreign policy issue. There are two opposing models. On the one side, 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 ITU, which could gradually replace ICANN. Russia and China belong to this group. On the other hand, 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.

The two sides clashed openly at the World Conference on International Telecommunications (WCIT) held in Dubai in December 2012 over a new International Telecommunications Regulations Treaty. After long and tense negotiations, a resolution was put to the vote. It was signed by 89 countries. 55 states refused to sign it, including the EU, its member states, and several EU strategic partners, i.e. the US, Canada, Japan and India. The other six EU strategic partners were among the signatories.

The West had for a long time been in agreement over internet governance, but small cracks have started to appear following the revelations of former NSA consultant Edward Snowden. Governments worldwide, including in Europe, condemned the US's espionage activities. US moral leadership over the internet has arguably come to an end. In the last few months, 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 February statement, the European Commission called for 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'.[87] In addition to the globalisation of ICANN and IANA functions, the EU seeks to empower ICANN's Government Advisory Council (GAC). 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 EU finds itself increasingly somewhere in the middle of the two sides, although incomparably closer to the US than to China or Russia. As a result, the EU is now trying to profile itself as an 'honest broker' in this debate,[88] and it could find potential allies in this endeavour among its partners. A recent study on internet governance identified 30 potential swing states that could play a pivotal role in this debate.[89] Five EU strategic partners figure in this list: Brazil, India, Mexico, South Africa and South Korea.

[87] European Commission, '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

[88] *Idem*.

[89] T. Maurer and R. Morgus, 'Tipping the scale: an analysis of global swing states in the internet governance debate', *Internet Governance Papers* 7, CIGI, May 2014.

Brazil is particularly interesting. Similar to the EU, it is trying to raise its profile on cyber issues. In April 2014, Brazil convened a major international conference on internet, NetMundial, with official representatives from 80 countries and from the private sector. Brazil also used this event to actively promote its own norms and policies. Although divergences emerged among Brazil, the EU and the US, the disconnect was much greater with Russia, China and other authoritarian countries.[90] The EU and Brazil could thus initiate a cyber *rapprochement* with the ambition to help shape the global internet governance agenda. Recently, the European Commission has proposed to set up a Global Internet Policy Observatory in cooperation with Brazil, with a view to promoting a more open and transparent internet governance.[91]

Assessing the partnerships

Cyber-security is probably the most transnational of all threats facing the EU.[92] Cyber-attacks can be carried out from anywhere in the world against systems located in any country, potentially using servers and computers located in yet another jurisdiction. International cooperation appears therefore essential, bilaterally and multilaterally. At the bilateral level, a fundamental objective of the EU's cyber-strategy is 'to reach out to its strategic partners to make our response more effective'.[93] However, the ten strategic partnerships are not all equally essential to the EU's cyber-security. Their core purpose varies from one partnership to another.

The EU-US partnership is by far the most developed in this policy area, and in essence the sole truly *strategic* partnership. The US is the only partner singled out in the EU's cyber-strategy. Reflecting this prime importance, there are multiple dialogues, contacts and agreements framing their cooperation, more than with any other partner. The WGCC is perceived as a 'good example of international cooperation',[94] which could perhaps inspire other partnerships. The EU-US partnership has led to concrete deliverables at the bilateral and global levels – multilaterally or in a triangulated manner. But in terms of cyber-security, the partnership is still incipient. Although some form of cooperation on cyber-security has existed for more than a decade, bilateral cooperation was stepped up only recently, in 2009, when Brussels and Washington raised the issue to the level of 'global concern'.[95] It holds a huge potential, but it must first overcome a serious trust deficit, notably following the revelations of Edward Snowden. The current negotiations over a bilateral agreement to ensure data protection is a key test to rebuild trust across the Atlantic and among citizens.

The partnerships with China and Russia rest on a different premise. By any standard, these two countries cannot be considered as strategic partners on cyber-security issues. Moscow and Beijing seen more as sources of cyber-insecurity than cyber-security, and reports regularly point to these two countries being the main source of cyber-attacks worldwide – although many cyber-attacks can also be traced back to the US or other Western countries.[96] There is a major trust

[90] C. Ballesteros, 'Net neutrality gets left out of Brazil online governance summit', *El Pais (English)*, 25 April 2014.

[91] Bendiek 2014, op. cit.

[92] Other major transnational threats identified in this series are nuclear proliferation, international terrorism and organised crime.

[93] Malmström 2012, op. cit.

[94] Council of the EU, 'Budapest conclusions', *Presidency conclusions of the Cybercrime Conference*, Budapest, 13 April 2011. Available online at: http://www.statewatch.org/news/2011/may/eu-council-budapest-conclusions-cyber-wall.pdf

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

[96] I. Steadman, 'Reports find China still largest source of hacking and cyber attacks', *Wired UK (online)*, 24 April 2013. Available online at: http://www.wired.co.uk/news/archive/2013-04/24/akamai-state-of-the-internet

deficit resulting from this situation (much deeper than with the US), which fundamentally hampers cooperation. As described above, there have been some instances of cooperation and more is foreseen. Nevertheless, it appears that the core purpose of the partnerships with China and Russia is less about deepening operational cooperation and more about taking bilateral confidence-building measures, with a view to keeping the lines of communication open, taming tensions, and making up for the weak multilateral framework.

The rest of the EU's partnerships are not as developed as the one with the US and not as difficult as those with China and Russia. Japan and Canada are mature partners, as illustrated by the EU-Japan MLA or the Europol-Canada operational agreement. Cooperation has mostly taken place on cyber-crime and CIIP. Very little cooperation has been reported at the bilateral level with the other five partners so far, despite the existence of structured dialogues on related matters.

Overall, the bilateral foundations of the EU's strategic partnerships in cyber-security remain weak and under-developed. The issue is still marginal in summit discussions and in ministerial meetings. There has been no specific joint statement on cyber-security, in contrast with such statements issued jointly with partners on terrorism or non-proliferation. The 2009 EU-US 'joint statement on enhancing transatlantic cooperation in the area of justice, freedom and security' indicated a joint commitment to addressing cyber-crime, but within a broader context of fighting transnational crime and terrorism.[97] The 2010 EU-India 'joint declaration on international terrorism' frames cyber-security in a narrow counter-terrorism context,[98] whereas the 2004 EU-Japan 'joint statement on cooperation on information and communication technology' makes only a brief mention of a 'more secure internet'.[99]

Until recently, cyber-security was not a major part of the bilateral agenda with most partners, including the US. There is little or no mention of cyber-security issues in most documents establishing the political priorities for each partnership. 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 only make brief references to cyber-security. Similar documents with other partners make no mention of cyber-security at all, namely 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.

Things are changing, however. Cyber-security has gained global traction in recent years and it is likely to become more prominent in the EU's 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.[100] The EU and Brazil announced at their latest summit that cyber-security and internet governance will be part of their next joint action plan.[101]

[97] EU-US, 'EU-US Joint Statement on "Enhancing transatlantic cooperation in the area of Justice, Freedom and Security"', 28 October 2009. Available online at: http://www.regeringen.se/content/1/c6/13/43/59/8542bc06.pdf

[98] EU-India, 'Joint declaration on international terrorism', Brussels, 10 December 2010. Available online at: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/118405.pdf

[99] EU-Japan, 'Joint Statement on Cooperation on Information and Communication Technology', 22 June 2004. Available online at: http://eeas.europa.eu/japan/docs/2004_ict_en.pdf

[100] EU-China, 'EU-China 2020 Strategic Agenda for Cooperation', 2013, op. cit.

[101] EU-Brazil, '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

The recent multiplication of bilateral dialogues with partners also suggests the rising importance of this topic in the partnerships' agenda. Four new dialogues have been launched in 2014 already with Brazil, Japan, South Korea and the US. There is now at least one dialogue on cyber-issues with each partner, which means that the fabric of the EU's cyber-diplomacy is thickening quickly. Yet, the scope and objective of each dialogue still largely depends upon the breadth of the partnership. Some dialogues are more results-oriented, for instance the one with the US, whereas others are more process-oriented, for instance those with China and Russia.

Beyond the purely bilateral dimension of these partnerships, cooperation also takes place at the multilateral level. However, the multilateral arena is highly contested – perhaps more than in any other security area. Two distinct visions of cyber-security and internet governance are in direct confrontation, dividing the EU's strategic partners. On the one side, some countries led by China and Russia seek to strengthen governmental control in the cyber-sphere. On the other side, a group of Western democracies, including the US, Canada and Japan work to maintain the multi-stakeholder system of internet governance and to develop effective international instruments addressing cyber-security issues. Several partners are caught somewhere in-between. They do not want to go as far as Moscow or Beijing, but they request more national oversight and demand the end of American stewardship over the internet, particularly in light of recent revelations of espionage. The EU has traditionally been part of the Western consensus, although it has recently somewhat distanced itself from the US, opening the door for more cooperation with partners such as Brazil or Mexico. There is anyway a large normative gap between the EU and its like-minded partners, on the one hand, and Russia and China, on the other hand. This gap was explicitly acknowledged in the EU Cyber-security Strategy, fundamentally limiting the scope of potential cooperation with non-like-minded partners.

The multilateral fabric is not only contested, but it is also pretty thin. The Budapest Convention is the only legally-binding instrument with regard to cyber-crime, but with around 50 signatories it is not a global instrument. Furthermore, not all strategic partners have signed it, with Russia and China firmly opposed to the instrument. Cooperation has been particularly difficult with the latter two countries. They have distinct views on cyber-security, while remaining engaged on these issues in multilateral fora whose objectives and principles are not always compatible with European ones, such as the Commonwealth of Independent States (CIS) or the Shanghai Cooperation Organisation (SCO). At the other end of the spectrum, the transatlantic partnership has been particularly effective at the multilateral level. The EU and the US regularly coordinate their positions in various fora, and they have also jointly launched the Global Alliance against Child Sexual Abuse Online, which was later joined by other like-minded partners, namely Canada, Japan, Mexico and South Korea.

The (inter-)regional level appears even less developed. Despite a commitment expressed in the cyber strategy to work more with regional organisations, such as the AU, ASEAN or the OAS, no cooperation has been reported at this level. In fact, cyber issues are not even mentioned in the 2007 EU-Africa Joint Strategy or in the 2012 EU Guidelines on East Asia.

In this context of thin and contested multilateralism, bilateral partnerships acquire particular importance to ensure effective cooperation when possible, mostly with like-minded partners, or to build confidence and try to progressively narrow the normative disconnect with others. The EU's multi-layered approach to cyber-security allows for interactions between bilateralism and multilateralism where there is a sufficient fabric of shared norms and objectives connecting the partners.

Conclusion

Spamming, hacking, espionage, cyber-attacks and cyber-terrorism are all rising practices across the web. As a result, most countries worldwide are now engaged in the fight against these security challenges. Issues related to cyber-security and cyber-governance are increasingly shaping the international agenda, as recently illustrated by the major NetMundial conference in Sao Paulo. Global partnering is becoming inevitable, and cyber-diplomacy is therefore intensifying.

This paper shows that the EU has actively built up its own cyber-capabilities over the last few years, including through the adoption of its own cyber strategy in 2013. More projects are in the pipeline, such as the development of a cyber-defence policy framework in 2014 at the request of the European Council. The EU is thus carving out its domestic and global cyber-profile. Its cyber-diplomacy is taking shape, with a multiplication of dialogues with international partners and a growing engagement at the multilateral level. Without doubt, the Union is progressively integrating and strengthening the global cyber-security fabric. Having said this, the EU's member states remain largely responsible for these issues, and they largely play their own cards at the international level. While the EU has become an important cyber player, there is still a long way to go before it becomes a cyber power.

Appendix

The purpose of this appendix is to offer synthetic information on each strategic partnership, to complement the main body of this paper. It covers the key documents defining the principles of cooperation (when they address cyber-security); relevant dialogues established to address cyber issues; and a brief assessment of each partnership. The information provided here is not comprehensive. Only the dialogues that deal with cyber-security issues on a regular basis are listed, leaving out other dialogues that could potentially address the issue in the future (this explains why summits or ministerial dialogues are not systematically mentioned).

EU-USA

Key documents:

- EU-US Joint Statement on 'Enhancing transatlantic cooperation in the area of Justice, Freedom and Security' (2009): http://www.regeringen.se/content/1/c6/13/43/59/8542bc06.pdf

Key dialogues:

- Summit (annual)
- Ministerial dialogue on justice and home affairs (twice a year)
- Working Group on Cyber-security and Cyber-crime (annual)
- Cyber dialogue (annual)
- Information and Society Dialogue (annual)
- EU-US-Russia dialogue on justice and home affairs (annual)
- EU-US-Canada meeting of senior officials on justice and home affairs (annual)

Brief assessment:

The EU-US partnership is by far the most developed, although the Snowden revelations have affected confidence between the parties. The partnership relies on a wide architecture of consultation mechanisms, leading to very concrete deliverables. Brussels and Washington also coordinate their positions effectively at the multilateral level. With regard to internet governance, they are broadly aligned although some divergences remain. When it comes to cyber-security, the partnership is characterised by asymmetry with regard to strategic thinking and capabilities – which is likely to grow further since the US is beefing up its capabilities.[102] As a result, the US is somehow steering the EU's response to cyber-threats, either through bilateral cooperation, or within NATO with regard to cyber-defence.

[102] E. Bumiller, 'Pentagon Expanding Cybersecurity Force to Protect Networks Against Attacks', *New York Times*, 27 January 2013.

EU-CANADA

Key documents:
None.

Key dialogues:
- EU-US-Canada meeting of senior officials on justice and home affairs (annual)

Brief assessment:
Cyber-security does not appear prominently on the bilateral radar screen. In spite of some instances of cooperation, notably via Europol, the partnership has delivered little. In fact, cooperation between the EU and Canada is largely framed in the broader framework of transatlantic relations, together with the US. Having said this, Canada is a constructive partner at the multilateral level, notably as a signatory of the Budapest Convention. The EU and Canada also jointly support the multi-stakeholder model of internet governance.

EU-MEXICO

Key documents:
- Mexico-European Union Strategic Partnership Joint Executive Plan (2010): http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/er/114467.pdf

Key dialogues:
- EU-Mexico dialogue on public security and law enforcement (annual)
- EU-Mexico working group on telecommunications

Brief assessment:
Although cyber-security was not on the bilateral agenda until recently,[103] both parties are starting to envision avenues for cooperation in this area. A new policy dialogue was established in 2013. Mexico is itself a prime target of cyber-crime and cyber-attacks; and its domestic criminal groups are increasingly developing online activities, notably for profiteering purposes.[104] Given this reality, Mexico has expressed interest in further cooperation on cyber-security, cyber-crime and internet governance.[105] Overall, however, cooperation remains limited.

[103] Interview with Mexican diplomats, Brussels, 4 May 2011.

[104] H. Stone, 'Mexico Moves into Cyber Crime', *Insight Crime*, 3 March 2011. Available online at: http://www.insightcrime.org/insight-latest-news/item/625-mexico-moves-into-cyber-crime

[105] EU-Mexico, 'Joint Communiqué', 2013, op. cit.

EU-BRAZIL

Key documents:
None.

Key dialogues:
- EU-Brazil dialogue on international cyber policy (annual)
- EU-Brazil information society dialogue (annual)

Brief assessment:
Cyber issues are only starting to become part of the bilateral agenda, as a new policy dialogue was established in 2014. Brazil is progressively shaping its global profile with regard to internet governance, promoting a less US-centred internet. This ambition, boosted by the Snowden revelations, took tangible form with the organisation of the major NetMundial conference dedicated to this issue in April 2014 in Sao Paulo, with representatives from more than 80 countries. As the EU and Brazil are trying to shape the cyber debate, this strategic partnership could gain prominence in the coming years, if the two sides manage to approximate their views and policies.

EU-SOUTH AFRICA

Key documents:
None.

Key dialogues:
- EU-South Africa ICT dialogue (annual)

Brief assessment:
Cyber-security seems to be inexistent on the bilateral agenda and no cooperation is in place at the moment. This could be partly explained by the fact that the relationship is still young and under-institutionalised and given that South Africa is just starting to develop its own strategy and policies to cope with this challenge.[106]

[106] 'South Africa: Cyber Security Policy Gets Cabinet's Thumbs Up', *AllAfrica*, 12 March 2012. Available online at: http://allafrica.com/stories/201203121310.html

EU-INDIA

Key documents:

- EU-India Joint Declaration on International Terrorism (2010): http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/118405.pdf
- The India-EU Strategic Partnership Joint Action Plan (2005): http://ec.europa.eu/enterprise/policies/international/files/eu_india_joint_action_plan_en.pdf

Key dialogues:

- Summit (annual)
- EU-India ministerial meeting (annual)
- EU-India political dialogue on cyber-security (annual)
- EU-India joint working group on information society (annual)

Brief assessment:

EU cooperation with India on cyber-security was originally framed in a narrow counter-terrorism context, in the 2005 joint action plan first and then in the 2010 joint declaration on international terrorism. As counter-terrorism efforts have lost their centrality on the international agenda while cyber issues have become increasingly important, the two issues have been distinguished with the recent launch of a separate dialogue on cyber-security. Although the EU and India stressed the 'importance of further dialogue' at their latest summit,[107] bilateral cooperation remains almost inexistent and the two sides are not aligned on internet governance issues.

EU-CHINA

Key documents:

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

Key dialogues:

- Summit (annual)
- High-Level strategic dialogue (annual)
- EU-China task force on cyber issues
- EU-China dialogue on IT, telecommunications and informatisation

Brief assessment:

The EU and China are both placing greater emphasis on ICT and cyber innovation in their domestic policies, notably in connection with their growth and development strategies (Europe2020 for the EU, and the 12th 5-year plan for China). There is thus a certain convergence of priorities, at least in the economic realm, which suggests that this policy area holds some potential for further cooperation. Yet, when it comes to narrower cyber-security considerations, China is perceived as an agent of insecurity, perhaps even a threat, not only in Europe but also in the US and in most neighbouring countries. China has developed its cyber capabilities (cyber-espionage, cyber-attacks and cyber-defence) with a view to supporting its strategy to become a major power, relying on a

[107] EU-India, 'Joint Statement', *EU-India Summit*, New Delhi, 10 February 2012. Available online at: http://eeas.europa.eu/india/sum02_12/docs/20120210_joint_statement_en.pdf

considerable force (probably the most extensive in the world) of cyber-spies and cyber-warriors.[108] This has certainly not appeased concerns from its partners. With regard to internet governance, the EU and China are also deeply divided. The strategic partnership in this field is thus limited, although certainly useful in terms of confidence-building measures. It is complemented by parallel cyber dialogues with some member states, including Germany.

EU-JAPAN

Key documents::

- An Action Plan for EU-Japan Cooperation (2001): http://www.mofa.go.jp/region/europe/eu/summit/action0112.html
- EU-Japan Joint Statement on Cooperation on Information and Communication Technology (2004): http://eeas.europa.eu/japan/docs/2004_ict_en.pdf

Key dialogues:

- Summit (annual)
- EU-Japan cyber dialogue
- EU-Japan dialogue on ICT policy (annual)

Brief assessment:

Although not particularly high-ranking on the political agenda, the EU and Japan have a well-developed and functioning cooperation on cyber-security at the bilateral level, but also at the multilateral level. The maturity of the partnership and the normative proximity between the two partners is visible in the fact that Japan signed the Budapest Convention, as well as in the fact that the two partners were able to conclude an ambitious MLA agreement. In addition, the EU and Japan are largely aligned on issues related to internet governance.

[108] K. Hille, 'Chinese military mobilises cybermilitias', *Financial Times*, 12 October 2011. See also M. Chansoria, 'Defying borders in future conflict in East Asia: Chinese capabilities in the realm of information warfare and cyber space', *The Journal of East Asian Affairs*, 26:1, 2012, pp. 105-128; M. Hjortdal, 'China's use of cyber warfare: Espionage meets strategic deterrence', *Journal of Strategic Security*, 4:2, 2011, pp. 1-24.

EU-SOUTH-KOREA

Key documents:

- Framework Agreement between the European Union and its Member States, on the one Part, and the Republic of Korea, on the other Part (2010): http://eeas.europa.eu/korea_south/docs/framework_agreement_final_en.pdf

Key dialogues:

- EU-South Korea Cyber Policy Consultation
- EU-South Korea information society dialogue (annual)

Brief assessment:

South Korea is often called the world's 'most wired' country, with the deepest internet penetration anywhere. It is a regular target of cyber-attacks.[109] As a result of this, Seoul has recently stepped up its efforts, notably launching a new cyber-security strategy.[110] There are thus good incentives for the EU and South Korea to cooperate in this policy area, as they have agreed in their Framework Agreement. Yet, this cooperation must still largely materialise.

EU-RUSSIA

Key documents:

- Road Maps for the Four Common Spaces (2005): http://eeas.europa.eu/russia/docs/roadmap_economic_en.pdf

Key dialogues:

- Permanent Partnership Council (several times per year)
- EU-Russia dialogue on information society (annual)
- EU-US-Russia dialogue on justice and home affairs

Brief assessment:

Russia is perceived more as a challenge or threat than as a partner in the area of cyber-security. Indeed, a great number of cyber-attacks or examples of cyber-espionage in Europe emanate from Russian territory, and these attacks appear to be politically motivated at times, for instance during the war with Georgia (2008) or in the current Ukrainian crisis. Little cooperation has therefore been reported at the bilateral level, whereas at the multilateral level confrontation is open. Russia refuses to sign the Budapest Convention despite being a full member of the Council of Europe, and it opposes the EU's views on internet governance. The partnership has therefore not delivered thus far, and it is unlikely to change in the near term given current political tensions. In contrast with the EU-China partnership, Brussels and Moscow have not yet felt the need to establish a bilateral confidence-building mechanism.

[109] J. Kim, 'S.Korea scrambles cyber defense for world's "most wired" country', *Reuters*, 14 June 2011.

[110] A. Valdez, 'South Korea outlines cyber-security strategy', *Asia-Pacific FutureGov*, 13 August 2011. Available online at: http://www.futuregov.asia/articles/2011/aug/13/south-korea-outlines-cyber-security-strategy/

The ESPO website (www.strategicpartnerships.eu)
is kindly supported by the Federal Foreign Office of Germany

FRIDE
A EUROPEAN THINK TANK FOR GLOBAL ACTION

EGMONT