The EU and its (cyber) partnerships

by Patryk Pawlak and Catherine Sheahan

The benefits of an open and accessible internet for growth and development have been acknowledged on numerous occasions. But as the potential of the digital economy for fostering innovation and creating new business opportunities grows, so too do the difficulties with protecting it. In February 2014, the European External Action Service presented the Friends of the Presidency on Cyber Issues with a Food for Thought Paper ('Further Strengthening European Cyber Diplomacy'). According to the document, 'the EU and its Member States should be in a position to present a coherent and comprehensive suite of policies which keep pace with the ever shifting international landscape, taking into account the strategic policy goals of other actors in the field'.

Strategic engagement with key regional partners is central to securing the Union's economic and political interests. It is therefore useful to clarify the scope of existing (as well as potential) cooperation with the EU's main strategic partners, especially those with regional influence, i.e. the United States, Brazil, South Korea, Singapore, South Africa, China, Egypt and India. Structured cyber consultations with Washington, Beijing and Delhi are already in place, and other less formal cyber dialogues – with South Korea and Brazil among others – are also underway.

Taking into account the EU's priorities as outlined in last year's Cyber Security Strategy, Figure 1 on page 3 highlights the performance of the Union's strategic partners in four main priority areas (fighting cybercrime, building resilience, strengthening diplomacy and developing defence capabilities) based on a set of proxy indicators presented in the Table on page 2.

Partnering in (fighting) crime

The rise of the internet economy has led to increased concern about cybercrime and cyber-espionage. The Boston Consulting Group estimates that the internet economy in G20 countries will grow by 8% each year for the next five years; in developing countries this figure is expected to be almost double that. At the same time, Europol estimates that victims of cybercrime lose around €290 billion each year worldwide, making internet crime more profitable than the global trade in marijuana, cocaine and heroin combined.

With regard to fighting cybercrime, the efforts undertaken by the United States, South Korea and Singapore provide valuable support for bringing the Union's digital agenda forward. The EU-US Working Group on Cybersecurity and Cybercrime, established

in 2010, aims to deepen the existing relationship in fighting organised crime and state-sponsored attacks. In 2012, the EU and the US launched the Global Alliance against Child Sex Abuse Online which now has 50 signatures (but none from the EU's other strategic partners). Cooperation between European and other law enforcement agencies has also contributed to solving several cases of cybercrime with an international dimension.

South Korea is one of the world's most 'wired' societies, with over 80% internet penetration. In search of new growth engines to drive the country forward, President Park Geun-hye plans to develop a 'creative economy' based on innovation and services. In light of this, Korea and France have recently announced strengthened cooperation in high-tech and futuristic sectors. At the EU-Republic of Korea Summit, in November 2013, leaders agreed to increase cooperation in cybersecurity, nano-safety, ICT, and cloud computing.

But Korea is also a good illustration of how technological advances and the internet economy are challenged by online illegal activities, as it also happens to suffer from high levels of cybercrime. Most recently, an IT contractor for the Korea Credit Bureau, a private credit rating agency, was arrested in January 2014 over the theft of personal data from 20 million credit card holders – around 40% of the population.

Internet users in Singapore, on the other hand, run a relatively low risk of exposure to intrusion or fraud, but the unlucky few suffer the highest losses *per capita* worldwide, according to the 2013 Norton Cybercrime Report. However, Singapore is actively seeking to position itself as a regional hub on cyber issues. It is hoped that the Interpol Global Complex for Innovation that will open in Singapore in 2014 will enhance collaboration between law enforcement agencies worldwide and boost national efforts to combat cybercrime. It may also provide scope for collaboration with the European Cybercrime Centre (EC3).

At the same time, the emerging economies' performance on cybercrime is quite worrying, given their importance for world trade. South Africa, in particular, has the third-highest number of cybercrime victims globally but also has limited cybercrime laws. In addition, although it is a signatory to the Budapest Convention, it has not yet ratified it. Egypt, another big regional player, has no cybercrime laws *per se* but this shortcoming is partly mitigated by the existence of laws regulating telecoms, e-signatures and consumer rights. The Information Technology Industry Development Agency (ITIDA) promotes a data protection framework and ensures copyright laws are enforced. Harnessing the benefits of the digital economy is particularly important for Egypt where the success of reforms aimed at improving societal development and human security will ultimately determine the success of political transformation in the country.

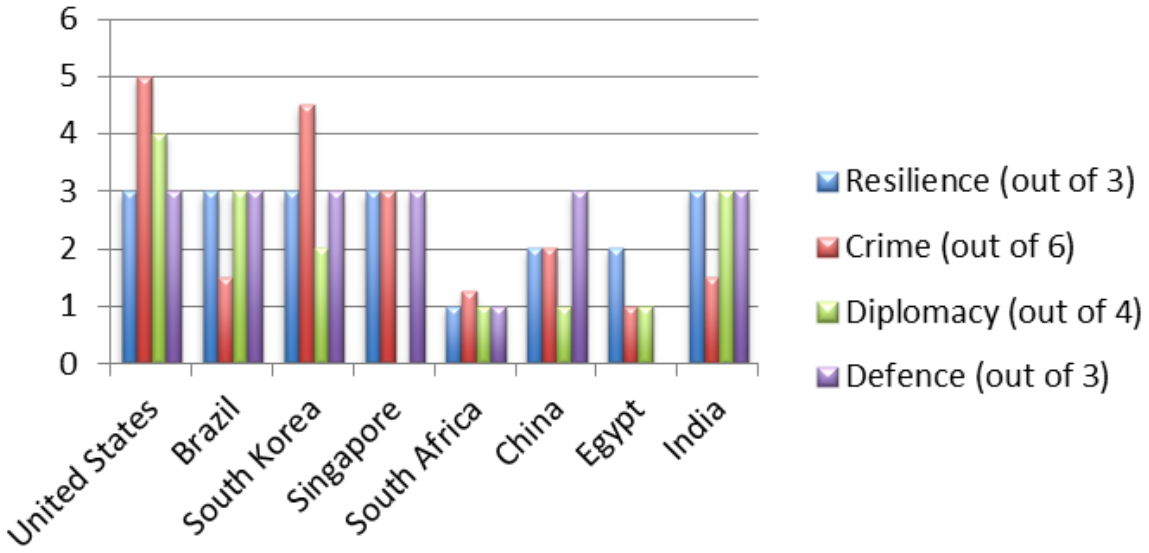
Table 1: Looking into the EU's cyber partnerships

Area	Proxy indicator
Resilience	• Cybersecurity strategy • CERT • Cyber awareness programmes
Crime	• Malicious attacks by origin rankings • Support and defence of the Budapest Convention • Participation in the Global Alliance against Child Sexual Abuse Online • Protection of intellectual property rights • Domestic cybercrime laws • Dedicated cybercrime centre
Diplomacy	• Freedom of expression: filtering and censorship • Protecting fundamental rights: International Covenant on Civil and Political Rights (ICCPR) • Cyber-related dialogue with the EU • Support for democratic and efficient multi-stakeholder governance: WCIT 2012
Defence	• Participation in cybersecurity exercises • Existing cyber defence framework • Military cyber defence organisations

Finding the (weakest) links

Ensuring resilience in cyberspace is another priority outlined in the EU Cyber Security Strategy. Computer emergency response teams (CERTs) are now seen as a crucial element for protecting critical infrastructure and building resilience. The efforts undertaken globally in this respect give grounds for optimism since

Figure 1: Cyber Partnerships: who to play with?



more security in India, China or the US will also help improve the EU's own security – even though their approaches may not always correspond with the Union's preferred option.

The United States, for instance, is the second biggest source of worldwide malicious attacks, according to the 2013 Kaspersky Security Bulletin. Even though this partly undermines its global standing, Washington's positions on cybersecurity shape international debates and, as a result, reflect and/or become global standards. The Framework for Improving Critical Infrastructure Cybersecurity, launched in February 2014, is transferable on a global level and can be used as a reference point for international cooperation between public and private sectors.

India launched its Cyber Security Policy in 2013, mostly in response to a significant number of attacks – like the recent infiltration of the control centre of Bharat Sanchar Nigam, a government-managed telecommunications company. Some key stumbling blocks that need to be addressed were highlighted during the country's first conference on cybersecurity and cyber governance in October 2013. The absence of a clear strategy, citizens' voice, and privacy laws prevent India from moving forward with policy commitments in a comprehensive way. In terms of concrete plans, 500,000 cyber-security professionals will be trained in the next five years to staff a National Critical Information Infrastructure Protection Centre.

Similarly, Singapore's National Cyber Security Master Plan is focusing its efforts on enhancing resilience of critical infrastructure and education, and boosting the pool of security experts and capabilities. To this end, it is increasing scholarships through the Infocom Development Authority and providing collaborative training programmes with private industry. It is also attracting private and public sector research projects. In February 2014 Israel's Aerospace Industries launched a Local Cyber Early Warning Research and Development Centre in Singapore.

China, on the other hand, has yet to formalise a cybersecurity strategy, despite 42.3% of its population using the internet (according to the World Bank). A recent meeting of the Central Internet Security and Informatisation Leading Group – composed of the leaders of various government departments – testifies to first efforts to deal with fragmented cyber prerogatives and a stronger profile in internet governance.

Syncing with the (wider) world

The backbone of the Union's cyber diplomacy is ensuring that its core values (i.e. democratic principles, human rights, and the rule of law) and its political, strategic and economic interests are protected. The year 2014 will see a number of important events that will significantly influence the future of cyberspace. In April, the Global Multistakeholder Meeting on the Future of Internet Governance will propose the internet governance principles. In October, the future role of the International Telecommunication Union (ITU) in areas related to internet governance will be debated at the ITU's Plenipotentiary Conference. Proposals for new intergovernmental mechanisms in internet governance will also be addressed in the Commission of Sustainable Technological Development. This implies that coordination of diplomatic efforts within the EU – but also with international partners – will become more important than ever.

Figure 1 suggests a relatively high convergence between the EU and the United States, Brazil and India, even though the overall picture is not so crystal clear. For example, despite the proximity of views, the US may prove an inconvenient ally for the EU – mostly as a consequence of the fallout from the NSA scandal. Yet the growing numbers of internet users and rate of internet penetration in other parts of the world means that such countries will have an increased interest, and role, in the future of internet governance.

Brazil's President Dilma Rousseff, in her speech to the 68th session of the United Nations General Assembly, highlighted that ICT cannot be the new battlefield between states and argued for increasing the UN role in preventing cyberspace from becoming a 'weapon of war'. A Brazilian-German initiative on the Right to Privacy in the Digital Age was adopted in November 2013 and was a direct response to the NSA revelations. Furthermore, Brazil took the lead on the Resolution on internet-related issues (co-sponsored by Argentina, China, India, Russia, Saudi Arabia and Uruguay) that was adopted at the UNESCO General Conference in late 2013.

China is also actively engaging in regional exercises and cooperation, most recently with the Republic of Korea at the Second China-ROK Internet Roundtable in Seoul. Exchanges have also taken place in the form of the Sino-US, Sino-Britain and China-Emerging Countries Internet roundtable conferences. Even though citizens have no formal right to privacy under the Constitution, data protection laws are being developed and supported by the EU-China Information Society Project (EUCISP). This four-year joint initiative of the EC and the Beijing government aims to promote economic and social reform in China through ICT.

Building (virtual) defence

The discussion about structuring relationships in the field of cyber defence is still at a nascent stage. Even though most countries do not hide their efforts at strengthening their own defensive capabilities, only a few governments worldwide have admitted to building up a cyber offensive arsenal. The lack of clarity about the thresholds differentiating defensive and offensive cyber capabilities is what complicates the picture – and the debate. This is why efforts towards formulating a set of binding confidence-building measures are of such importance. The Cyber Security Confidence Building Measures adopted by the OSCE in 2013 and the consensus reached by the third UN Group of Government Experts (GGE) leave room for moderate optimism.

In terms of military capabilities, most countries have included cyber-related provisions into their defence framework. The evidence suggests that Egypt is one of a few states analysed that does not have a formal cyber defence framework or a military cyber defence organisation (like the US Cybercommand or Brazil's Cyber Defence Centre). On the whole, Egypt's cybersecurity has proceeded on uncertain ground of late: the use of the 'internet kill switch' during the Arab Spring raises questions of whether it could happen again – even under a different leadership – and pinpoints cyberspace as unreliable for economic activities.

Interestingly enough, regional defence partnerships are growing between Europe's strategic partners. In January 2014 India and South Korea agreed to enhance collaboration between their national security structures and to launch a Cyber Affairs Dialogue. Brazil has also launched a number of bilateral cyber partnerships in Latin America – inter alia with Argentina – aimed at the creation of an organisation for analysing cyber defence cooperation.

Friends with (fringe) benefits

This quick overview of cyber-related policies in different parts of the world suggests that the EU is destined for marriages of convenience. While some countries can support the Union's efforts in fighting crime and building resilience, their compatibility on the normative dimension of EU cyber diplomacy is often rather limited. It must also be acknowledged that, despite the clear need for collective action(s), the EU is in direct competition with several countries concerning the future governance of the internet and/or global standards.

Nevertheless, a number of initiatives can contribute to improving collective cyber capabilities and provide the basis for EU engagement with other parts of the world. There is no single 'good' model for securing cyberspace – therefore, the exchange of good and bad practices between individual countries and regional organisations may help streamline ongoing efforts. Given different levels of development across the world, a collective effort in capacity building is of paramount importance in both preventing the emergence of safe havens and ensuring that developing countries can fully harness the benefits of ICTs for development. Finally, the potential of regional organisations for stimulating cross-regional cooperation needs to be further explored.

Patryk Pawlak is a Senior Analyst and Catherine Sheahan is a Junior Analyst at the EUISS.