BRIEF ISSUE 32 2013


# Cyber world: site under construction

by Patryk Pawlak

The Union's cyber security policy may still be in its infancy and hampered by difficulties, but the EU could yet become a key player in the field – if it plays its cards wisely. While the US has been seriously hit by the scandal surrounding the secret NSA surveillance programmes, the struggle over how to frame internet governance goes on and, more than ever, needs core stakeholders capable of defending freedom, democracy and the rule of law in cyberspace.

The EU's longstanding commitment to those values in its foreign policy and unquestioned leadership in data protection mean it is well placed to play a significant role therein. At the same time, the EU and its member states have recently accelerated efforts to increase their cyber-defence capabilities so as to secure Europe against malicious cyber-attacks (like those carried out against the office of European Council President Herman van Rompuy in June 2012). To be truly effective, they may have to be able to play, at the same time, the roles of policeman, diplomat and regulator.

## A new cyber world order?

Two concurrent debates about the governance of cyberspace provide the backdrop against which the EU seeks to strengthen its role and capabilities.

First, the growing dominance of digital communication networks has brought to the fore two sharply conflicting visions about the future of the internet. A group composed primarily of liberal democracies (including the EU and US) argues that the multi-stakeholder approach bringing together governments, the private sector, civil society and technical experts should continue to provide the basis for internet governance. This stance is opposed by a group of 'cyber-sovereignty' advocates (including China and Russia) who wish to either retain or claw back more governmental control of cyberspace. The two sides clashed openly at the World Conference on International Telecommunications in Dubai in December 2012. The biggest bones of contention were (i) bringing internet governance under the regulatory framework of the International Telecommunications Union (*de facto* taking it away from the private sector and putting it into government hands); and (ii) giving states the authority to label certain content as spam (and therefore use this as a pretext to curb free speech).

The second element in the debate concerns the application of existing international law to cyber conflicts. Europe's engagement in building international consensus is required here because the EU and its member states can be both targets and originators of cyber-attacks. Reducing possible sources of tension requires cross-border coordination of

diplomatic, law enforcement and technological expertise. Moreover, uncertainty related to cyber-attacks – what constitutes an 'attack', how definitely the identity of an attacker (and its possible links with state structures) can be ascertained – can be resolved only if the international community develops a common understanding and situational awareness. Several international organisations have tried to develop confidence-building measures but, so far, efforts to bring all members of the global community on board have failed. The most prominent attempt to date – by the UN Group of Governmental Experts, in 2010 – resulted in a report on the application of international law and standards to cyberspace. A year later the Shanghai Cooperation Organisation (in particular SCO members China, Russia, Uzbekistan and Tajikistan) made its own submission to stimulate the discussion about international norms and rules regulating the conduct of states in cyberspace. The most recent initiative, undertaken under the aegis of the OSCE in 2012, was a package aimed at preventing a cyber-war – but it collapsed after Russia refused to sign up to the conclusions. Instead, Moscow advocates a universal cyber-convention that would codify reasonable standards of state behaviour.

Moving from the *status quo* – characterised by a patchwork of cyber-governance instruments [Table 1] – towards new regulations or changes in existing ones is necessary to reduce the uncertainty that affects and limits state and non-state actors alike. The direction in which the regulatory system may evolve will have significant security, economic and societal implications for Europeans. The EU thus needs to monitor developments closely and use its unique position to influence these debates.

## Add-ons 'made in the EU'

The Union's Cyber Strategy endorsed by member states on 25 June 2013 sets out five strategic priorities: (i) achieving cyber resilience; (ii) drastically reducing cybercrime; (iii) developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP); (iv) developing the industrial and technological resources for cyber security; and (v) establishing a coherent international cyberspace policy for the EU with a view also to promote core values. The strategy also reiterates the Union's commitment to existing international laws regulating cyberspace, including the International Convention on Civil and Political Rights, the Geneva Conventions and the principles enshrined in the Budapest Convention on Cybercrime. The European External Action Service, in particular, is tasked with ensuring the protection of freedom and human rights in the digital world, coordinating capacity-building assistance, strengthening the accountability and stability of the internet, and maintaining relations with partners and international organisations.

**Table 1: Who does what in cyberspace (non-exhaustive)**

| | **Regional and global level** | **EU level** | | |
|---|---|---|---|---|
| | | *European Commission* | *EEAS* | *Member states, EU agencies and other institutions* |
| **Cybercrime and justice** | UN, Interpol, Council of Europe | DG Home, DG Justice | Conflict Prevention and Security Policy | Europol, Eurojust, FRA, EDPS, MS, Council (e.g. Friends of Presidency), EP (e.g. LIBE) |
| **Cyber resilience** | OECD, ITU, UNIDIR, UNICRI | DG Connect, DG Enterprise, DG Research | EUMS, CMPD | ENISA, EU-CERT, MS (CERTs), Council (e.g. Friends of Presidency), EP (e.g. ITRE) |
| **Cyber diplomacy** | Council of Europe, NATO, OSCE | DG Devco EuropeAid | Conflict Prevention and Security Policy | MS, Council (e.g. Friends of Presidency, PSC) |
| **Cyber conflicts** | ITU, UNODC, NATO, OSCE | DG Enterprise, DG Research | EUMS, CMPD | EDA, MS, Council (e.g. Friends of Presidency, PSC, EUMC) |

Source: Author's compilation based on official documents and online sources.

The Cyber Strategy, however, also makes clear that achieving these objectives will not be possible without international cooperation. Cybercrime cannot be combated effectively without police and intelligence services working across borders. Promoting freedom of the internet and other core values cannot be achieved without engagement at the global and regional level. Yet international engagement, in order to be credible, needs to proceed in lockstep with the development of cyber capabilities aimed at building resilience and raising awareness. These three dimensions – law enforcement, regulation and diplomacy – are vital for strengthening Europe's collective say on cyber governance.

- *The EU as a policeman: combating the dark side of the internet*

The EU's contribution to the fight against organised crime, including its extensive network of law-enforcement partnerships on cybercrime and related issues, provides the backbone for its international role. The Union strongly

supports the principles for fighting online crime set out in the Budapest Convention on Cybercrime and engages in capacity-building efforts designed for law enforcement. It has successfully carried out cross-border operations targeting child sexual-abuse file-sharing networks (Operation Icarus) and child sexual exploitation (Operation Atlantic), and countering credit/debit card fraud. On top of that, the 'Cyber Atlantic' exercise – involving more than 20 countries and conducted jointly with the US Department of Homeland Security in 2011 – focused on a simultaneous attack on critical infrastructures in several countries.

In addition to international efforts, the EU focuses on improving its own capabilities. In institutional terms: it has set up a European Cybercrime Centre (EC3); launched a network of national centres of excellence for cybercrime training, research and education (already operational in seven member states and under development in three more); and designed cybercrime training materials for law enforcement under the auspices of the European Cybercrime Training and Education Group hosted by Europol. The EU has also established a network of law enforcement 'contact points' – operational 24/7 – which brings together officials with cyber expertise who are capable of providing urgent assistance.

In terms of legislative initiatives, the Foreign Affairs Council of 23 July 2013 approved the directive on attacks against information systems. This legislation defines – and establishes criminal sanctions for – basic offences or attacks against critical infrastructure and information systems. Worth mentioning also are an obligation on member states to respond within eight hours to urgent requests for help, and an obligation to collect statistics on cyber offences. Member states now have time until September 2015 to transpose these new rules into their national legal systems.

- *The EU as a diplomat: building trust and capacities*

Improving access to broadband communication in the developing world is necessary to achieve the economic and social benefits that the internet brings, including improved access to education and healthcare and, in the longer term, reducing poverty. This, however, cannot be achieved without concurrent efforts to improve the security of cyber infrastructure. For this reason HR/VP Ashton has highlighted the need for new cyber-capacity programmes and called for better coordination of existing initiatives. The EU is already involved in cyber-capacity building efforts, such as training law enforcement experts and providing funding for ICT-oriented projects (e.g. in Georgia).

Another important dimension for harnessing the EU's diplomatic potential is through confidence-building measures (CBMs). Despite attempts by international organisations like the UN, OSCE or NATO, multilateral solutions are still missing. Ambiguity remains with regard to what constitutes an aggression and to what extent existing international law applies to cyber-attacks. This is why the creation of a common vocabulary with internationally recognised definitions for gradations of attacks and potential targets remains a priority. In the absence of an overarching framework, the Union's bilateral initiatives – like the EU-China Cyber Task Force, or scientific and law-enforcement cooperation with Russia – may provide a platform for building trust.

'Moving from the *status quo* – characterised by a patchwork of cyber-governance instruments – towards new regulations or changes in existing ones is necessary to reduce the uncertainty that affects and limits state and non-state actors alike.'

The EU's external action would be curtailed without the ability to effectively secure the conduct of CSDP missions and operations. A study to assess the cyber-defence capabilities of member states recently carried out by the European Defence Agency revealed a rather mixed picture on cyber-intelligence gathering and incident-response capabilities. Nevertheless, several efforts are underway, including developing Cyber Defence Situational Awareness for CSDP operations and Cyber Defence Training Needs Analysis. The European Council on security and defence in December 2013 may also provide an opportunity to further develop some key concepts (i.e. the need to integrate cyber defence into the planning and conduct of CSDP missions, training and exercises).

- *The EU as a regulator: fostering cyber-resilient societies*

Given the existing patchwork of international cyber regulations, the EU's own experience as a collective supra-national regulator is another strong point. Ever since the creation of the Single Market, the EU has been at the forefront of international harmonisation and standard-setting (including on digital communication), as well as the eradication of safe havens. Yet a 2012 Eurobarometer survey revealed that almost one-third of Europeans do not feel confident that their privacy is protected when using the internet. Defending the EU's international position at a time when some of its fundamental values and norms are being constantly challenged will be all the more difficult without first proving that a European model works for its own citizens.

This is why EU initiatives, including the Digital Agenda for Europe, focus on strengthening the resilience of systems and the Union's internal capacities by involving all relevant stakeholders. The EU is currently discussing a directive on network and information security (NIS) that would see member states establish competent authorities at the national level, set up Computer Emergency Response Teams (CERTs) and adopt national NIS strategies and cooperation plans. Furthermore, government institutions, operators of critical infrastructure (such as energy, transport or banking) and key internet enablers (e-commerce platforms, social networks) will be responsible for performing risk assessments and adopting appropriate measures. Contrary to the position preferred by some in the cyber community (the private sector in particular), the EU has put forward its own model for transparency that obliges private entities to report any incidents with a significant impact on core services provided.

The EU has been the unquestioned leader on data protection since 1995, when the Data Protection Directive (DPD) was adopted. The directive – currently under revision – provides a legal framework regulating transnational data exchanges between public and private authorities: it has constituted a benchmark for international data flows for almost a decade. The DPD was used to ensure (with varying degrees of success) that the security considerations which drove most of the counterterrorism policies introduced around the world after the 9/11 terrorist attacks did not undermine civil liberties and, in particular, citizens' right to privacy. With several new regulations adopted over the past ten years – especially those addressing the use of personal information for security purposes – the European data protection regime remains the most robust in the world.

## Towards 2015

A secure and safe digital environment is a necessary condition for reaping the benefits of ubiquitous access to the internet. With the number of devices connected to the internet expected to reach 15 billion by 2015, addressing the threats posed by malicious cyber activities is a clear priority. This is why the Union's recent initiatives in developing cyberspace policies and capabilities are most welcome. Hardly any other actor on the international stage has capacities, experience and credibility comparable to those of the EU in this domain. Its recent focus on cyber issues sends a signal that Europe is willing to participate in (and possibly shape) the ongoing debate. This is particularly important in view of the World Summit of the Information Society, scheduled in 2015, when major decisions about the future of the internet (including security) will once again be on the table.

***Patryk Pawlak is a Senior Analyst at the EUISS.***



QN-AK-13-032-2A-N | ISSN 2315-1110