EUSC EU-China Security Cooperation: performance and prospects

Policy paper series, Autumn/Winter 2014

The EU's Approach to Cyber Security

George Christou, University of Warwick

Introduction

Cyber security policy has been on the European Union (EU) radar for many years. It established the European Network and Information Security Agency (ENISA) in 2004 in order to facilitate a movement towards shared knowledge and improved 'best' practice among Member States and there was a clear security (sub) dimension connected to the evolution of the EU's Information Society agenda. The issue was elevated up the EU's political agenda in 2007, with NATO, the EU and other actors forced to radically rethink their approach following the Distributed Denial of Service (DDoS)[1] attacks on Estonia's public and private infrastructure. Subsequently, the EU's policy has developed and been underpinned by the need to achieve the objectives it has set for itself in the Digital Agenda for Europe[2] (2010), and equally as significant, the driving force of such an agenda, the Europe 2020 strategy. In addition, it has recognised that as a security issue the protection of cyber security is borderless and has highlighted in its policy documents, including numerous Internal Security Strategies, the European Guidelines and Principles for Internet Resilience document (March 2011) and its Cybersecurity Strategy (2013) the importance of global partners and working in partnership with them to address the civilian and military aspects of cyber security challenges.

The increasing use of and reliance on the Internet for the everyday lives of EU citizens in the social, economic and political realm and the constant development of information and communications technology is seen as critical to the growth strategy of the EU – and therefore, cyberspace[3] is an asset that needs to be protected so that it remains 'open and free [with] the same norms, principles and values that the EU upholds offline' (EU Cybersecurity strategy, p. 2). To this end, the EU published its Cybersecurity Strategy on 7 February 2013, and accompanying this, an ambitious Directive on Network and Information Security (NIS Directive) proposed by the European Commission (DG Connect), that sought, among other things, to make mandatory the reporting of significant cyber incidents across all critical infrastructure sectors as well as enablers of key internet services (NIS Directive 2013). The Strategy represented the first ever attempt by the EU to set out clear priorities for the protection of cyberspace. Prior to this, the policy was dispersed across many Regulations and Directives, and whilst an approach existed, key dimensions (in particular cyber defence) were missing and it was certainly not as coordinated as required for the construction of an effective security ecosystem for cyberspace (see Klimburg and Tirmaa-Klaar 2011).

Whilst the EU Cybersecurity Strategy in itself does not make the EU approach less fragmented, it is certainly seen as starting point for realising a more coherent, coordinated and integrated approach across the EU machinery, and indeed outwards towards and within the relevant international institutions, transnational networks, regional bodies and nations states. At the time of writing the strategy is still in its infancy – only operational for just over one year – and it is far too early to make a categorical judgement on its achievements.[4] Indeed, the NIS Directive is still being debated within

the relevant EU institutional machinery (Council and European Parliament) with agreement in the Council of Ministers unlikely to be reached until the end of 2014. The progress made thus far, however, can certainly provide us with an idea of how far the EU has travelled in addressing threats in cyberspace, and indeed for the main purposes of this paper, whether the underlying norms, principles and logics that underpin the EU approach allows for cooperation and convergence with China on issues relating to the security of cyberspace. On the latter, the EU-China 2020 Strategic Agenda for Cooperation (2013) certainly points to promoting, as a joint objective, 'a peaceful, secure, resilient and open cyber space' and 'promoting mutual trust and cooperation through such platforms as the EU-China Cyber Taskforce' (p.4). This paper will aim to shed light on whether the norms and logics of security that underpin the EU and China approaches to cyberspace will actually enable this to happen in practice – and if so, in what specific areas of cyber security and through which instruments, processes and platforms.

The paper will be structured in the following way in order to achieve its main objectives. Section I will provide a brief overview of the conceptual landscape and its relevance for understanding the EU's cyber security development. Section II will sketch out the EU's approach, logics and values that underpin it and the proposed instruments for EU cyber security policy. Section III will then provide a review of how the EU has sought to deal with cyber security threats in practice, focusing on the international dimension in particular. This section will touch upon the issue of the EU's international engagement and cooperation with China in relation to cyberspace. The final section will conclude by providing thoughts on the potential for future cooperation between the EU and China on cybersecurity.

Understanding the EU in cyber security: approaches and concepts

The academic literature on the EU's action in cybersecurity, thus far, has been sparse, even though there has been a rapid growth in the topic more broadly, with scholars taking a variety of approaches to explain and provide a better understanding of the development of cyber security policy. The majority of work that does exist is focused on the US and other geographical areas (e.g. see Kshetri, 2013 on the Global South), with no comprehensive theoretically driven analysis of the EU in cyber security (for this, see Christou 2015, forthcoming). In terms of the existing literature, a variety of approaches have been used to analyse the topic, ranging from traditional national strategic and managerial approaches (for example, Libicki 2007, 2009; Clarke and Knake 2010), to historical approaches (Carr 2009) and 'terrorist' oriented approaches (Wiemann 2006; Colarik 2006). Such approaches focus more on the real and present danger of cyber threats and potential management of the risks associated with them; in other words, on how to fight the cyber enemy or achieve the 'cyber peace' (Clarke and Knake 2010). More conceptually, methodologically, and theoretically informed works have employed governance (regulatory) approaches (Mueller 2010, Brown and Marsden 2007), pragmatic, eclectic, comparative approaches (Karatzogianni 2006, 2009; Eriksson and Giacomello 2010), innovative mixed-method approaches (Deibert *et al.* 2012), and more critical approaches that attempt to assess the extent to which cyber policy has become securitised (Dunn Cavelty 2007, 2008; Bendrath *et al.* 2007).

The most widely used concept for understanding both the EU and nation state approaches to cyber security – and their ability to act in cyberspace – has been that of cyber power (Klimburg and Tirmaa-Klaar 2011; Betz and Stevens 2011; Klimburg 2011; Nye JR. 2010; Kramer *et al.* 2009). This concept has been defined and utilised in a variety of ways. For example, Joseph Nye Jr. (2010), in an attempt to demonstrate the types of behaviour, instruments and resources that can be used in the cyber

with the support of the Lifelong Learning Programme of the European Commission

world by state and non-state actors alike, defines cyber power, in its wider sense, as 'the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power' (2010, p.4). He further differentiates between physical and information instruments, and hard and soft power in cyber space, and gives examples of how they can be used inside (intra cyberspace power) and outside (extra cyberspace power) (See Table 1 below).

Table 1: Instruments of power in cyberspace

	Intra cyber space	Extra cyber space
Information Instruments	Hard: Denial of Service attacks Soft: Set norms and standards	Hard: Attack SCADA systems Soft: Public diplomacy campaign to sway opinion
Physical Instruments	Hard: government controls over companies Soft: Infrastructure to help human rights activists	Hard: Bomb routers or cut cables Soft: Protests to name and shame cyber providers

Source: Joseph Nye Jr. (2010, 5)

Others, whilst also essentially still focusing on the 'state' and cyber power, have recognised its complexity and understand it as 'the variety of powers that circulate in cyberspace and which shape the experiences of those who act in and through cyberspace' (Betz and Stevens 2011, p.44). In other words, they recognise that cyberspace is fluid, and that a multiplicity of both state and non-state actors, from individual citizens to states, global institutions and networks, can exert cyber power at any point in time in order to exploit the opportunities offered to them by cyberspace. To this end, they seek to extend the conception of cyber power identifying four distinct forms: Compulsory, which is the use of direct coercion by one cyberspace actor in an attempt to modify the behaviour of another (hard power such as the Anonymous attack on FBI systems); Institutional, which 'involves the indirect control of a cyberspace actor by another, principally through the mediation of formal and informal institutions (soft power such as setting norms and standards); Structural, which 'works to maintain the structures in which all actors are located and which...permit or constrain the actions they may wish to take with respect to others to whom they are directly connected (soft power related to how cyberspace itself can facilitate or constrain the actions of actors); and finally, Productive, which 'is the constitution of social subjects through discourse mediated by and enacted in cyberspace, which therefore defines the 'fields of possibility' that constrain and facilitate social action (soft power such as a states' construction of the 'hacker' as threat).

Klimburg (2011) also defines three dimensions of cyber power which he considers important: 1) coordination of operational and policy aspects across governmental structures; 2) coherency of policy through international alliances and legal frameworks; 3) cooperation of non-state cyber actors. Contrary to Nye Jr., he argues that of these dimensions the third is the most significant given the nature of the Internet and cyberspace; the majority of control comes from business and civil society and the capability of the state is limited to indirect rather than direct influence. In this context, Klimburg, drawing from the Integrated Capability Model (see Klimburg and Tirmaa-Klaar 2011, p.11),

with the support of the Lifelong Learning Programme of the European Commission

posits the need for an integrated approach to cyber security, whereby, in his view, 'the non-state sector must be induced to cooperate with government', going on to argue that 'the most important dimension of cyber power is thus the ability to motivate and attract one's own citizens, an inward-focused soft-power approach that is fundamental for creating a 'whole of nation' cyber capability' (2011, p.43, my emphasis). He points out that the US has been slow to realise how important an integrated approach to cyber power is, and argues that Russia and China both 'have highly capable and highly visible non-state cyber capabilities that interact with their governments' (ibid, p.43-44).

In applying this concept to the EU, Klimburg and Tirmaa-Klaar concluded in their report for the European Parliament that there was 'no concept of projecting 'hard' or 'soft' power via an integrated approach to cyber power, and therefore for helping to define international cyber security around the core values of the Union' (2011, p.37). Whilst the Cybersecurity Strategy (2013) has addressed some of the report's recommendations it is an open question whether the EU can or even should develop all dimensions of cyber power – and indeed whether 'hard' cyber power thought of in conventional national security terms is actually compatible with the EU's core norms and values. This point is particularly salient if we consider the post-PRISM (e-spying) revelations that certain EU Member States (e.g. UK, Sweden) were complicit in mass data surveillance of citizens (and elites for that matter) – in contravention of established EU laws on privacy/data protection and codes of conduct – or norms – among 'friends' in Europe.

It can be argued that the EU, in order to stay true to its own norms and values (see below) – needs a security of resilience approach (Christou 2015, forthcoming) and a certain specific type of cyber power – not the conventional, direct (hard, offensive) cyber power often defined by many scholars in the US, and exercised most by those states, democratic and authoritarian, that approach the issue of security in cyberspace through the logic of cyber sovereignty, but a soft power, that builds on Klimburg's three dimensions as well as institutional and productive cyber power, and that fosters a climate of trust, mutual cooperation, collaboration and information sharing among the many stakeholders that are active in cyberspace. This is even more imperative in the post-Snowden era – where the results of the power struggle in cyberspace have been clear for all to see in terms of the consequences of a 'national security' first logic which has relegated rights, privacy, freedom and democracy to a status of irrelevance – and which has very much contradicted the EU's vision of a cyberspace that is open, safe, democratic and secure. In this sense then, Dunn Cavelty (2013, p.3) argues that the EU needs to develop a very specific 'soft' power, built on internal resilience and its core values, in order to ensure that its stated normative vision for the governance of the Internet and indeed cyberspace is projected and achieved in the global arena. Such an approach, unfortunately, might very well be the main obstacle to convergence with China on many aspects of cyber security, in particular given that the general Chinese approach is very much driven by the national 'sovereign' interest – and with this, hard cyber power and traditional modes of security thinking (see below).

The EU approach to cyber security

The EU's approach to cyber security has evolved over time in an ad hoc and fragmented manner, incorporating the institutional logics and therefore approach of those actors within the machinery that have been responsible for the development of the different strands of cyber security 'policy'. These strands can largely be divided into: cybercrime and cyber attacks, dealt with in the main by Directorate General Justice and Home Affairs; Network and Information Security (NIS), which is essentially made up of Critical Infrastructure Protection (CIP) and Critical and Information Infrastructure Protection (CIIP) and dealt with by Directorate General Connect (previously DG

with the support of the Lifelong Learning Programme of the European Commission

Information Society); and finally, and much more visible in the EU's Cybersecurity Strategy document (2013), a cyber defence element that would fall under the responsibility of the CSDP machinery and in particular the European External Action Service (EEAS). These strands, in turn, embed the EU's approach with a legal logic (enforcement), economic logic (Internal Market) and security logic (CSDP) (see Robinson 2013), reflecting the complexity of the cyber security domain, and the potential difficulty for ensuring that the EU constructs a coherent and coordinated internal policy that can also be projected outwards in global deliberations on norms and principles for cyberspace behaviour. Furthermore, the Cybersecurity Strategy delineates the above strands as strategic priorities, and adds a further two dimensions: a) Developing the industrial and technological resources for cyber security b) Establishing a coherent international cyberspace policy for the EU in order to promote core EU values.

The EU's approach to cyber security is not without normative foundation, and is underpinned by broader principles and guidelines that have been defined for Internet stability and resilience, and indeed Internet governance more broadly (European principles and guidelines 2011; EU Cybersecurity strategy 2013; Internet Governance: the next steps 2009, 2014). With regard to the latter, the EU approaches the global Internet as a public or collective good that should be available to and accessible by all. That is, there is a normative view that use of the Internet should not be restricted or limited to any citizen, the exception being with regard to measures and instruments that are used in order to prevent harm to others. Furthermore, when it comes to cyber security, it is clear that EU core values, laws and norms are as central to online activity as they are offline and that 'Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union...' (EU Cybersecurity Strategy 2013, p.4).

Beyond this, there is also a very clear EU idea on the governance model of choice for the Internet and cybersecurity policy more specifically, that of multistakeholderism (see Internet Governance: the next steps 2009; and EU Cybersecurity Strategy 2013). This model, of course, is not without controversy. Whilst the multistakeholder vision is born from the very complexity of the Internet in terms of the many actors involved in its management and use – and is shared by many 'Western' states (e.g. US, Japan, Canada, and Australia), it is highly contested by those states (e.g. Iran, Russia, China, India) that consider a) the US to hold too much power over the management of the Internet b) themselves to be under-represented in the existing global Internet governance institutions (Internet Corporation for Assigned Names and Numbers, Internet Governance Forum) and that wish to see much more governmental involvement in cyberspace through the ITU – that is, a traditional intergovernmental rather than a multi-stakeholder approach.

The importance of the involvement of all stakeholders is also reflected in the EU's principle of shared responsibility for the effective security of cyberspace. In this sense, this runs throughout the additional principles and guidelines that the EU presents as critical for Internet resilience and stability, including that of improving education and raising awareness, internal EU cooperation and mutual assistance, creating a strong ICT industry in Europe (ensuring diversity of products), good risk-management and the construction and uptake of open standards with security and privacy built in from the design phase (European principles and guidelines 2011).

Significant in the context of this paper is the salience the EU places on the global context and international cooperation. The EU is all too aware that any EU principles on cyber security do not exist in a vacuum, and that, without cooperation and collaboration with international public and private partners to create global principles compatible with EU values, the EU's attempts to construct

with the support of the Lifelong Learning Programme of the European Commission

its own resilient cyber security policy will be fundamentally weakened, as will the stability and interoperability of the Internet. Global disagreement and contestation, for example, on the role of technical standards, data protection and privacy, who should control and regulate the Internet, and the appropriate legal conventions for fighting cybercrime (e.g. the Budapest Convention) can undermine any attempt to create a secure cyberspace for all. Whilst the EU primarily supports a multistakeholder approach for the governance of the cyber world, it is also clear that public authorities have an important role to play in providing a normative and legal framework for the activities of the all stakeholders. In other words, the EU supports within the multistakeholder umbrella a specific type of public-private partnership, where public authorities should decide (in consultation with relevant stakeholders) on the appropriate modes and forms of governance and regulation (i.e. incentives) and where the private sector has an important day-to-day role in the management of the Internet (European principles and guidelines 2011; EU Cybersecurity strategy 2013, p.3). In this sense, the EU, in particular in the post-Snowden era, has also supported a greater role for the Governmental Advisory Committee in ICANN, to give it a greater decision-making role in policy on Internet governance.[5]

The EU Cybersecurity strategy: practice, progress and challenges

Where then, does this leave us with the EU's overarching approach to cyber security and indeed the instruments at its disposal to achieve it? What have been the successes and limitations thus far and what are the implications for cooperation and convergence with China? Unlike the United States (US) (and indeed China and Russia), where there is a primary emphasis on a national security (threat) logic and therefore deterrence and militarisation as the central strategy (hard power), the EU takes a fundamentally different approach to cyber security which is focused on building resilience to ensure rapid recovery from cyber attacks, building the necessary capacities to resist cyber attacks, and fighting cybercrime (soft power). Whilst one of the EU's strategic priorities is to address its lack of military and intelligence infrastructure and capability in cyber security, this is clearly the least developed strand (on this, see Robinson 2014) and is not as important as the other four priorities that focus on non-military aspects that each seek to build the necessary capacities and partnerships to create an effective culture of cyber security within and beyond the EU (see Bendiek 2014).

The EU has numerous instruments, institutions and agencies at its disposal with regard to pursuing its Cybersecurity Strategy. These range from voluntary arrangements (to ratify the Budapest Convention), incentives, dialogue, platforms for cooperation and coordination, to more formal, mandatory requirements, such as the proposed NIS Directive that compel the relevant stakeholders to report cyber incidents or to ensure the privacy and protect the data of EU citizens. There is a dynamic debate within Europe between the relevant stakeholders on the efficacy of mandatory reporting for creating a culture of cyber security collaboration, and at the time of writing the evidence suggests that the original NIS Directive will be significantly watered down by the European Parliament and the Council before any agreement is reached. Whilst there seems to be widespread agreement that a public-private model of governance is desirable, the question is open with regard to which instruments work best to achieve a resilient EU cyber security system or indeed allow the EU to develop effective institutional and productive (soft) cyber power. Nevertheless, there has been some progress on achieving certain aspects of the Cybersecurity Strategy (see Table on Implementation of the Cybersecurity Strategy 2014), and in particular with regard to the work of the European Cybercrime Centre (EC3) which supports EU law enforcement authorities to prevent and

with the support of the Lifelong Learning Programme of the European Commission

investigate cross-border cyber crime (EC3 Report 2014; European Cybercrime Centre – one year on, 2014).

Given the aims of this paper, the rest of this section will focus on the most relevant aspects of the EU's overall approach in relation to its international outlook and projection, and draw out the potential difficulties and opportunities for EU-China cooperation on cyber security issues. The EU's international activity thus far has focused on building bilateral relationships,[6] engaging in international platforms (such as the London conference with follow-ups in Budapest and Seoul) and relevant regional and international fora (ITU, OECD, ICANN, IGF, Council of Europe), as well as enhancing its relationship with other relevant international organisations (NATO) in the development of its Cyber Defence Policy Framework. Specific joint actions with China on cyber security have been limited to commitments within the broader goals of the EU-China 2020 Strategic Agenda for Cooperation (2013), with, thus far, limited results. For example, whilst the EU-China Task Force established to enhance cooperation on cyber issues has met twice, the last occasion being hosted by the EEAS in October 2013, the reported result from the EU was that whilst it 'provided a good opportunity to deepen cooperation...[it] highlighted inevitable differences between our approaches to cyberspace' (Table on Implementation 2014, p.25). These differences have indeed manifested themselves not just in the bilateral realm, but also in discussions and negotiations over establishing global norms for the governance and security of the Internet, in particular in relation to cyber war and cyber crime.

The CoE (Budapest) Convention on Cybercrime illustrates this point very well. Whilst this is problematic within the EU – not just externally – as not all Member States have ratified and indeed implemented it across Europe,[7] this is further exacerbated by the global dimension to this issue with those that contest it, which includes China and Russia, as well as certain developing countries. Indeed they have stated their clear opposition to ratifying the Convention due to the concern that it would undermine national security culture, which is certainly problematic to achieving a global security of resilience given the number of Internet users in these countries and the fact that they are the alleged source of many cyber security breaches and attacks in recent years. Whilst the Global Project on Cyber Crime has been established for just this purpose – to promote the Convention beyond Europe – and has had partial success in terms of certain countries in Asia and Latin America drawing on the Convention and implementing legislative reforms based on it,[8] others still posit and propose a view, grounded on alternative norms and principles. The Shanghai Cooperation Organization (SCO) nations (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan) for instance, have an agreement in place – the *International Information Security Agreement* – that emphasizes a primary role for national security and the primary role of the state in controlling information technology and managing risks and threats. Moreover, it sees Western nations and their dominance of the information space as a major threat to them, their socio-political systems and cultural way of life (Goldsmith 2011, p.4). Similar to other norms and tools invented in Europe and the EU then, the Convention embodies many useful principles for ensuring effective cyber security, but agreement and implementation beyond Europe will be difficult given the different approach to these matters taken by China and other members of the SCO.

This contestation also plays out with regard to the call for global norms for cyber security behaviour. If we compare the principles (norms) advocated by the EU, US, UK and ITU to those of the SCO, then we can again observe different logics at play with regard to the norms advocated for state behaviour in cyber space (Healey 2011a), whilst also noting some element of convergence. Although the SCO agreement did not explicitly discuss norms, it emphasised 'state control'; indeed in previous proposals from Russia there was a clear and predictable steer to the limitation of cross-border flows

with the support of the Lifelong Learning Programme of the European Commission

of information because of the impact that this might have on the culture of national security. Developments since then have seen a very broad consensus emerge between Russia, China, the US, EU and the UK on some of the general principles and norms for governing cyber security such as confidence-building, but such discussions have avoided the more controversial issues of content and information control (see UN Group of Government Experts Report to the Secretary General).

In September 2011, members of the SCO (Russia, China, Tajikistan and Uzbekistan) proposed that the UN Secretary General facilitate a dialogue around their new draft proposal, the 'International Code of Conduct for International Security'. This was drafted as a formal document of the 66th session of the UN General Assembly, with the express purpose of it being used to reach a consensus on international norms of behaviour for the Internet. This Code of Conduct (below Table 2) raises a series of basic principles, which at first glance do not seem divergent from what is being advocated by the EU. For example, complying with the UN charter, international cooperation, full respect for rights and freedoms in cyberspace, protecting critical infrastructure and a commitment to ensure supply chain security are all 'norms' that chime with many of the principles proposed by the EU in its Cybersecurity Strategy. Despite this, however, a deeper look at the security logics behind the proposal also raises potential points of concern for many that advocate a multi-stakeholder approach to cyber security and the preservation of freedom of access, expression, and information. Sceptics have argued, for instance, that the emphasis on promoting the 'establishment of a multilateral, transparent and democratic international management of the Internet', and the expected commitment to '...prevent other states from using their resources, critical infrastructures, core technologies and other advantages, to undermine the right of the countries...to independent control of ICTs, or to threaten other countries' political, economic and social security', are underpinned by a sovereign logic of control rather than freedom.

Table 2: International Code of Conduct for Information Security (SCO)

1.To comply with the UN Charter and universally recognized norms governing international relations, which enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all states, respect for human rights and fundamental freedoms, as well as respect for diversity of history, culture and social systems of all countries.	2. Not to use ICTs including networks to carry out hostile activities or acts of aggression and pose threats to international peace and security. Not to proliferate information weapons and related technologies.
3. To cooperate in combating criminal and terrorist activities which use ICTs including networks, and curbing dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment.	4. To endeavour to ensure the supply chain security of ICT products and services, prevent other states from using their resources, critical infrastructures, core technologies and other advantages, to undermine the right of the countries, which accepted this Code of Conduct, to independent control of ICTs, or to threaten other countries' political, economic and social security.
5. To reaffirm all states' rights and responsibilities to protect, in accordance with	6. To fully respect the rights and freedom in information space, including rights and freedom

with the support of the Lifelong Learning Programme of the European Commission

relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage	of searching for, acquiring and disseminating information on the premise of complying with relevant national laws and regulations.
7. To promote the establishment of a multilateral, transparent and democratic international management of the Internet to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet.	8. To lead all elements of society, including its information and communication private sectors, to understand their roles and responsibilities with regard to information security, in order to facilitate the creation of a culture of information security and the protection of critical information infrastructures.
9. To assist developing countries in their efforts to enhance capacity-building on information security and to close the digital divide.	10. To bolster bilateral, regional and international cooperation, promote the United Nations' important role in formulation of international norms, peaceful settlement of international disputes, and improvement of international cooperation in the field of information security, and enhance coordination among relevant international organizations.
11. To settle any dispute resulting from the application of this Code through peaceful means and refrain from the threat or use of force.	

Source: http://news.dot-nxt.com/2011/09/13/china-russia-security-code-of-conduct

For the first of these Codes, the promotion of the UN to take a more active role in Internet governance, where China has greater weight and influence in terms of voting behaviour, could potentially lead to traditional state governance and Balkanization of a spate of national Internet spaces, rather than multi-stakeholder governance. This also has implications for the notion of creating a cooperative culture of cyber security if other actors are sidelined in favour of a state-led, constructed, and enforced approach. For the second and third of these 'Codes', given the previous commitments by members of the SCO to limit information flows if it impacts on their own security culture, alongside the perceived dominance of the US in controlling the Internet, there are concerns that it would provide justification for repressive regimes to limit free speech and access to independent external news sources, as happened during the Arab uprisings in Egypt and Libya (see also Gjelten 2010). Moreover, it might also provide an excuse to introduce draconian laws and tighter controls on access, use and dissemination of information, as well as freedom of expression that might threaten 'national security' (see Healey 2011b; Bendiek 2014, p.12). Whilst at the level of discourse the meaning of the Codes put forth by the SCO seem compatible with the norms of the EU, the interpretation and practice only point to diametrically opposed approaches and logics with regard to cybersecurity. Thus even basic objectives and goals agreed on cyber security, such as confidence and trust building measures, become difficult to implement in practice when cybersecurity in China means suppressing undesirable content, and creating tools to keep the cyber enemies at bay. Finally, there are also further concerns about what is not visible in the Codes of Conduct. These include no commitment to control patriotic hackers supported by states that are seen to be at the centre of cyber conflict, and of which Russia and China are seen as critical sponsors. Second, there is no Code that calls for all states to sign up and be bound by the laws of armed conflict: the EU, US and UK are already committed to this norm, but Russia and China are not, which

with the support of the Lifelong Learning Programme of the European Commission

leaves open many of the traditional questions related to proportionality and the legitimacy of certain targets (Christou 2015, forthcoming).[9]

Conclusions

The prospects of deeper cooperation between the EU-China remain at the level of discourse rather than practice at this moment in time. Whilst there is certainly an agreement within the EU-China 2020 Strategic Agenda for Cooperation (2013) to enhance mutual trust and understanding, their approaches to security in cyberspace seem too diametrically opposed for any concrete action to be taken, whether this be on cross-border information sharing required for cybercrime, norms that should govern behaviour in cyberspace, or the issue of a free and open Internet for all. The Snowden affair has also brought the issue of rights and democracy under closer scrutiny and increased pressure for the EU to ensure that the rights of Europeans online are promoted both internally and across borders. This, in turn, has raised an additional challenge with regard to role of cyber espionage in protecting national security.

If deeper cooperation is to be achieved between the EU and China in the realm of cyber security in the near future, then established platforms such as the Task Force must produce a realistic agenda that is reflective of the differences between the EU (soft power) and China (hard power), but that does not compromise the norms and principles of either with regard to the Internet. This is difficult but not impossible, and there is momentum and renewed emphasis on cyber security in the EU, with its evolving cybersecurity strategy, and among the Chinese elite, through the newly founded governmental body the *Central Internet Security and Informatisation Leading Group.* China is certainly engaging in regional exercises on cyber security – and this might be a way forward for developing the EU-China relationship in this realm. Collaboration and trust can also be built through concrete initiatives such as the EU-China Information Society Project (EUCSIP),[10] and the involvement of Chinese institutes and organisations in cyber related research and innovation, in particular through the Horizon 2020 programme.

References

Bendiek, A.(2104) 'Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance and Data Protection', SWP Research Paper, RP5, March 2014, Berlin.

Bendrath, R. Eriksson, J. and Giacomello, G., (2010) 'From 'cyberterrorism' to 'cyberwar', back and forth: how the United States securitized cyberspace', in Eriksson, J. and Giacomello, G., (eds) (2010) International Relations and Security in the Digital Age. London and New York: Routledge.

Betz, D. and Stevens.T., (2011), Cyberspace and the State: Towards a Strategy for Cyber-Power, The International Institute for Strategic Studies. Oxon: Routledge.

Brown, I. and Marsden C.T., (2007), 'Co-regulating Internet Security: the London Action Plan', http://essex.academia.edu/ChrisMarsden/Papers/700007/Co-regulating_Internet_security_the_London_Action_Plan (accessed October 2011).

Carr, J. (2009), Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media.

with the support of the Lifelong Learning Programme of the European Commission

Christou, G (2015, forthcoming) Cyber Security in the European Union: Resilience and Adaptability in Governance Policy, New Security Challenges Series, Houndmills, Basingstoke: Palgrave Macmillan

Clarke R.A. and Knake R.K. (2010) Cyber War: The Threat to National Security and what to do about it. New York: Harper Collins.

Colarik, A.M. (2006), Cyber terrorism: Political and Economic Implications, IGI Publishing.

Deibert, R.J., Palfrey J.G, Rohozinski, R., and Zittrain, J., (eds.) (2011) Access Contested: Security, Identity and Resistance in Asian Cyberspace. Cambridge: MIT Press.

Dunn Cavelty, M. (2007), 'Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate, Journal of Information Technology and Politics, 4(1), 19-35.

Dunn Cavelty, M. (2008), Cyber-Security and Threat Politics: US efforts to secure the Information Age. London and New York: Routledge.

Dunn-Cavelty, M (2013) 'A Resilient Europe for an Open, Safe and Secure Cyberspace', Occasional Papers, No.23, The Swedish Institute of International Affairs.

European Commission (2013), 'Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace', Brussels, 7.2.13, JOIN (2013) 1 FINAL

European Commission (2009), 'Internet Governance: Next Steps', Communication from the Commission from the European Parliament and the Council, Brussels, 18 June, COM (2009) 277 final.

European Cybercrime Centre – one year on (2014), European Commission, Press Release, Brussels, IP/14/129, 10 February 2014.

European Cybercrime Centre: First Year Report, Available at: https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report (accessed 24 March 2014).

European Principles and Guidelines for Internet Resilience and Stability, March 2011. Available at: http://ec.europa.eu/danmark/documents/alle_emner/videnskabelig/110401_rapport_cyberangreb_en.pdf (accessed 11 March 2014).

EU-China 2020 Strategic Agenda for Cooperation (2013). Available at: http://eeas.europa.eu/delegations/china/press_corner/all_news/news/2013/20131123_en.htm (accessed 25 March 2014).

Gjelten, T., (2010), Seeing the Internet as an 'Information Weapon', 23 September, Available at: http://www.npr.org/templates/story/story.php?storyId=130052701 (accessed 12 March 2014).

Goldsmith, J., (2011), 'Cybersecurity treaties: A Sceptical View', Future Challenges Essay. Hoover Institution, Stanford University.

Healey, J. (2011a), 'Comparing Norms for National Conduct in Cyberspace', 20th September, Available at: http://www.acus.org (accessed 12 March 2014).

Healey, J.(2011b), 'Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms, 21 September, Available at: http://www.acus.org (accessed 12 March 2014).

with the support of the Lifelong Learning Programme of the European Commission

Klimburg, A. (2011) Ruling the Domain: (Self) Regulation and the Security of the Internet, Austrian Institute for International Affairs, April 2011.

Klimburg, A. and Tirmaa-Klaar, H. (2011) 'Cyber war and Cyber security: challenges faced by the EU and its Member States', DG for External Policies, Policy Department, European Parliament, April 2011.

Kramer, F.D., Stuart Starr and Larry K.Wentz, (eds) (2010) Cyber Power and National Security. Washington D.C.: National Defence UP.

Kshetri, N. (2013), Cybercrime and Cybersecurity in the Global South, New Political Economy Series. Houndmills, Basingstoke: Palgrave Macmillan.

Libicki, M.C. (2007) Conquest in Cyberspace: National Security and Information Warfare. NewYork: Cambridge University Press.

Libicki, M.C. (2009) Cyber Deterrence and Cyber War, Rand Corporation.

Mueller, M.L. (2010), Networks and States: The Global Politics of the Internet, M.I.T. Press.

Nye, J. (2010), 'Cyber Power', Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010.

Robinson, N., (2013) 'The European Cyber Security Strategy: Too Big to Fail?', Available at: http://www.rand.org/bog/2013/02/the-european-cyber-security-strategy-too-big-to-fail.html (accessed 11 March 2014).

Robinson, N., (2014) 'EU cyber-defence: a work in progress', European Union Institute for Security Studies (accessed 20 March 2014).

Table on the Implementation of the 'Cybersecurity Strategy of the European Union : A Open, Safe and Secure Cyberspace', (JOIN(2014)1), Working Document, 28 Feb 2014. Available at: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-strategy-high-level-conference-0 (accessed 24 March 2014).

United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201, Study Series 33, 2010.

Wiemann, G. (2006) Cyberterrorism: How Real Is the Threat'. Washington DC, United States Institute of Peace.

Endnotes

[1] DDoS refers to an attack where an individual computer is flooded with information from many other computers, forcing it to slow, shut-down or malfunction. Such attacks usually occur through 'botnets' of hijacked computers (Tirmaa-Klaar and Klimburg 2011, 8)

[2] Reviewed in 2012. See http://ec.europa.eu/digital-agenda/

[3] Cyberspace is understood for the purpose of this chapter as 'The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks

with the support of the Lifelong Learning Programme of the European Commission

connected to it, which does not exist in any physical form' (I**SO/IEC**, ISO/IEC 27032 Guidelines for Cybersecurity, 2011)

[4] There was a review of the Implementation of the EU Cybersecurity Strategy after one year at a High Level Conference in Brussels on 28 February 2014. See http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-strategy-high-level-conference-0

[5] There has also been greater support by the Commission for an inclusion of democratic states such as India and Brazil in such structures in order to improve transparency and representation.

[6] Established with India and being examined in 2014 in relation to Japan, South Korea, Brazil and Taiwan.

[7] EU Member States that have not ratified the Budapest Convention at the time of writing include: Luxembourg, Greece, Poland, Ireland and Sweden

[8] See Council of Europe, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp)

[9] The Tallinn Manual (2013) provides guidance on governmental reactions to cyber attacks, but is not without its controversy both in terms of the ambiguity of its underlying principles and the way it was constructed (without experts from non-NATO states).

[10] This four year project between the EU and the Beijing government aims at to promote economic and social reform in China through ICT. For final report and results see: http://egov.iist.unu.edu/download/EU-China-Information-Society-Final-Report.pdf

with the support of the Lifelong Learning Programme of the European Commission