EU-Japan Security Cooperation: Challenges and Opportunities

University of Essex

A project co-funded by the University of Essex and the Erasmus+ Programme of the European Union

Online paper series, Spring/Summer 2017

The EU's Approach to Cybersecurity

George Christou, University of Warwick

Introduction

While the EU's recognition of computer crime and information and computer security can be traced back to the late 1970s, it is more recent events that have seen cybersecurity[1] elevated up the EU's political agenda. Indeed, NATO and the EU were forced to radically rethink their approach to securing cyberspace following the Distributed Denial of Service (DDoS)[2] attacks on Estonia's public and private infrastructure in 2007. Subsequently, the EU's cybersecurity policy has developed and been underpinned by the need to achieve the objectives it has set for itself economically, in relation to the Digital Agenda for Europe (2010) and Digital Single Market Strategy (European Commission 2015b), and the driving force of such an agenda, the Europe 2020 strategy. 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] – as 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" (European Commission 2013b, 2).

In this context it was acknowledged that for the digital market and thus growth to flourish, consumers had to have trust that the products and services provided on the Internet were secure. This culminated in the creation of a contractual Public-Private Partnership (cPPP) between European industry (represented by the European Cyber Security Organisation) and the European Commission, the main objective of which is to offer better protection against cyber attacks in Europe and strengthen the competitiveness of the European cybersecurity sector through fostering "cooperation at early stages of the research and innovation process and to build cybersecurity solutions" across and within different sectors (energy, finance, health, etc.) (European Commission 2016). Ideas for harmonising the EU cybersecurity market through a certification framework (standards) have also been discussed within EU policy circles.

Beyond the strong economic (threat) logic driving EU cybersecurity policy, the EU has also been driven by a legal and security logic to protect cyberspace against cyber criminals and perpetrators that seek to attack – for political and well as economic reasons – European critical (information) infrastructures, and other public and private entities. To this end, the issue of cybercrime and cybersecurity has been addressed in numerous strategy documents, including the EU Internal Security Strategy (2010), the Stockholm Programme (2010-2015) the European Agenda on Security

(European Commission 2015a), the Joint Framework on Countering Hybrid Threats (European Commission and EEAS 2016), and the EU's Global Strategy (Council of the EU 2016). Furthermore, the European Principles and Guidelines for Internet Resilience document (European Commission 2011) and its Cybersecurity Strategy (European Commission 2013b) highlight the importance of global partners and working in partnership with them to address the civilian and military aspects of cybersecurity challenges.

The EU's Cybersecurity Strategy is reflective of the differentiated way in which the cyber threat is perceived – the central pillars of prioritised action broken down into: Cybercrime; Network and Information Security; Cyber Defence; Developing the industrial and technological resources for cybersecurity; and Establishing a coherent international cyberspace policy for the EU in order to promote core EU values (European Commission 2013b:4-5). The Strategy represents 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. Although the Strategy in and of itself has not automatically imbued the EU with the required vertical and horizontal coherence in its actions, it has proved useful in focusing minds on the steps necessary for a coordinated and integrated approach across the EU ecosystem to emerge, and indeed in dialogue with the relevant international institutions, transnational networks, regional bodies and nations states. Coordinative mechanisms such as the inter-institutional Horizontal Working Party on Cyber Issues (formerly the Friends of Presidency Group) and the increased role of the EEAS in cyber diplomacy are just two examples of how the EU has sought to develop its (internal and external) coherence in cybersecurity. At the centre of creating a more resilient European digital environment – and proposed in conjunction with the Cybersecurity Strategy of the EU (CSSEU), is the Network and Information Security Directive (NIS Directive). Adopted in July 2016 by the European Parliament, it is the first piece of legislation on cybersecurity that seeks to ensure a minimal institutional capability for reporting cyber incidents across Member States and therefore managing the risk associated with cyber attacks. To this end, and again with the aim of improving coherence, it "also establishes a 'Cooperation Group' between Member States, to support and facilitate strategic cooperation as well as the exchange of information, and to develop trust and confidence" (European Commission 2016).

It can be argued that the EU has made a great deal of progress since penning the CSSEU,[4] agreeing certain essential building blocks such as, for example, the NIS Directive (2016), operationalising the European Cybercrime Centre (EC3, 2013), agreeing more robust legislation on data protection and privacy through the General Data Protection Regulation (GDPR) and finally, extending the mandate (2009) and accelerating the review (2016) of the European Network and Information Security Agency (ENISA, established in 2004); the latter driven by the dynamic nature of the cybersecurity landscape and the potentially more urgent need to support EU member states become cyber resilient, beyond facilitation. This said, a great deal of diversity, incoherence and asymmetry still remains in terms of the implementation of the central tenets of the EU's Cybersecurity Strategy, and challenges certainly remain in relation to: establishing sustainable trust-based, collaborative relationships (public-public, public-private, private-private); education, skills, resource and training; and establishing global norms, standards and rules of the game to address threats in cyberspace.

The main aim of this paper will be to illuminate further the underlying perceptions, norms, principles and logics that underpin the EU approach with the objective of providing a contextual platform for exploring the prospect for cooperation and convergence with Japan on issues relating to the security of cyberspace. 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 cybersecurity development. Section II will sketch out the EU's approach, logics and values that underpin it. Section III will then focus on EU cyber threat perceptions, cybersecurity instruments and practices and the international dimension in particular. The paper concludes by providing thoughts on the EU approach and what this potentially implies for future cooperation with what is considered to be a 'like-minded' state, Japan.

The EU as power in cybersecurity

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 cybersecurity policy. The majority of work that does exist is focused on the U.S. and other geographical areas (e.g., see Kshetri 2013 on the Global South), with no comprehensive theoretically driven analysis of the EU in cybersecurity (for this, see Christou 2016b). 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 cybersecurity – and their ability to act in cyberspace – has been that of cyber power (Klimburg and Tiirmaa-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 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" (2010:4). 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).

Table 1 *Instruments of power in cyberspace*

	Intra cyber space	*Extra cyber space*
Information Instruments	Hard: Denial of Service attacks Soft: Set norms and standard	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 2011:44). 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 state's 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, drawing from the Integrated Capability Model (see Klimburg and Tiirmaa-Klaar 2011: 11), Klimburg posits the need for an integrated approach to cybersecurity, 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" (2011:43, *my emphasis*). He argues that Russia and China both "have highly capable and highly visible non-state cyber capabilities that interact with their governments" (*ibid*.: 43-4).

In applying this concept to the EU, Klimburg and Tiirmaa-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 cybersecurity around the core values of the Union" (2011:37). 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 (in particular GCHQ in the UK) were complicit in mass data surveillance of citizens (and elites for that matter) – in contravention of established EU laws on data protection/privacy 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 2016b) 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 (2013:3) 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. This sort of soft power does not contradict the EU's ambition to develop its cyber defence capabilities – as such capabilities involve 'cyber self-protection and assured access to cyberspace to enable conventional military activity' (Roehrig and Smeaton 2013:24) – and not the development of cyber offensive weapons that create for some, greater vulnerability and insecurity (cybersecurity dilemma) rather than security in cyberspace (Dunn Cavelty 2014).

The EU approach to cybersecurity

The EU's approach to cybersecurity 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 cybersecurity policy.

These strands can largely be divided into: cybercrime and cyber attacks, dealt with in the main by Directorate Generals Justice and Home; Network and Information Security (NIS) that encompasses Critical Infrastructure Protection (CIP) and Critical and Information Infrastructure Protection (CIIP), and dealt with predominantly by Directorate General Connect; and finally, 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 cybersecurity 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 cybersecurity b) establishing a coherent international cyberspace policy for the EU in order to promote core EU values. The EEAS has played a leading role in the latter as internal coordinator of the EU's external positions in bilateral and multilateral fora, and in some cases as the EU representative in issues of cyber diplomacy (see Christou 2016b).

The EU's approach to cybersecurity 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 Commission 2011, 2013b, 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 cybersecurity, 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" (European Commission 2013b: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 European Commission 2009; and European Commission 2013b). 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., the U.S., Japan, Canada, and Australia), it is highly contested by those states (e.g., Iran, Russia, China, India) that consider a) the U.S. 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 International Telecommunication Unions (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 Commission 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 cybersecurity 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 its own resilient cybersecurity policy will be fundamentally weakened, as will the stability and interoperability of the Internet. Global disagreement and contestation – with no like-minded states – 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 Commission 2011; 2013b: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 the Internet Corporation for Assigned Names and Numbers (ICANN), to give it a greater decision-making role in policy on Internet governance.[5]

Such an approach bodes well for the positive cooperation with Japan in cybersecurity – considered by the EU to be like-minded normatively. Japan is signatory to the Budapest Convention and has, for example, in its Cybersecurity Strategies of 2013 and 2015, emphasised the importance of working in multilateral fora and in cooperation bilaterally with states and regional organisations in order to ensure freedom and the basic values of democracy, rights and the rule of law are upheld in cyberspace. Moreover, whilst Japan has been categorised as a 'nascent cyber power' because of it movement to securitise and militarise its responses to the cybersecurity challenges that it has faced – that is, it has sort to acquire and develop hard power in terms of cyber defence (Kallender and

Hughes 2016:2) – this has been normatively in line with other like-minded partners such as Australia, the U.S., the EU, and NATO and in contradistinction to states such as China, that are perceived to contravene the laws of cyberspace (*ibid*.: 15). Indeed, the increase of Advanced Persistent Threats (APTs) in the cyber domain against Japanese industry and public sector institutions has often been attributed to China (but also, even though less so, to North Korea and Russia). As well as the ratcheting up of Japanese cybersecurity policy in response to this, it has led to intensive and enhanced cooperation with like-minded partners, in particular (and predominantly with) the U.S., but also with EU member states that are seen as leaders in cybersecurity (France, the UK) and with the EU since October 2014, when the EU-Japan cyber dialogue was launched in recognition of the necessity for a safe, open and secure cyberspace and promoting cooperation on cyberspace through exchanges of experience and knowledge.

The Cybersecurity Strategy of the EU: threat perceptions, practice and challenges

The EU's Global Strategy (Council of the EU 2016:22) highlights cybersecurity as a priority (threat) area and points to the importance of fostering a 'common cybersecurity culture' in order to raise preparedness for cyber disruptions and attacks. What we have seen emerging in the EU is a system of cybersecurity governance – driven primarily by the CSSEU, and which is underpinned by interweaving economic, legal and security logics, and distinct even though inter-related mandates: Justice and Home Affairs, Internal Market and CSDP and within multiple spaces – national, regional and global (Christou 2016b). That is, the EU perception of cybersecurity – or more broadly, the importance of information and communications technologies – has evolved and been accelerated over time from a matter of threat to the *economic* goals of the EU in its ambition to create and complete its Single Market project, to the security implications of increasing trends in computer-related and high-tech crime in the 1990s, and significantly, in the 2000s, enhanced measures – legally, procedurally and in terms of strategy, in reaction to the threats of external cyber attacks from inside and outside – from terrorists, hackers, states, and cybercriminals – putting at risk not only the cybersecurity resilience of EU institutions and member states, but also an array of EU objectives relating to its Information Society and Digital Market ambitions (see Christou 2016a).

The EU's cybersecurity logics and threat perceptions, then, have driven the *differentiated* set of instruments, agencies and institutions that are available to achieve its objectives in cyberspace – underpinned by a normative approach towards the Internet that aims to secure freedom, access and openness for all. Unlike those countries that might be considered to be hard powers in cyberspace (e.g., the U.S., China and Russia), where there is a primary emphasis on a national security (threat) logic and therefore deterrence and militarisation as the central strategy, the EU takes a fundamentally different approach to cybersecurity 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 cybersecurity, 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 cybersecurity 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, and platforms for cooperation and coordination (such as the NIS PPP and the cPPP), to more formal, mandatory requirements, such as the agreed NIS Directive (2016) and the GDPR (2016) which, respectively, compel the relevant stakeholders to report cyber

incidents and ensure the privacy and protect the data of EU citizens. There has been some progress on achieving certain aspects of the Cybersecurity Strategy (European Commission 2013a) in particular in terms of agreeing legislation such as the NIS directive, and with regard to the work of the European Cybercrime Centre (EC3) which supports EU law enforcement authorities to prevent and investigate cross-border cyber crime (Europol 2014; European Commission 2014). Here, novel operational governance mechanisms such as the Joint Cybercrime Task Force (J-CAT) have evolved to combat the threat of transnational cybercrime (Christou 2017). The European Network and Information Security Agency (ENISA) has also provided essential support to member states in providing guidance on EU NIS legislation (e.g. on reporting incidents), and in alerting and preparing member states through cyber exercises the minimum national requirements and capabilities needed to respond to any cyber attack. In cyber defence, whilst the least mature in terms of the EU's pillars, member states did agree in 2012 on the EU Concept for Cyber Defence in EU-led operations, allowing operational commanders to create and maintain situational cyber awareness. In the same year, EU Defence Ministers also agreed to put cyber defence on the Pooling and Sharing agenda to facilitate joint working on training and education. The European Defence Agency (EDA) as lead agency in this field has also made some progress in realising the five key areas agreed in the European Council Conclusions in December 2013 (European Council Conclusions 2013), in particular in relation to cyber training, education and exercise opportunities for member states.

One of the five key priorities in the CSSEU is to foster "international cooperation in cyberspace … together with relevant international partners and organisations, the private sector and civil society" (European Commission 2013b: 14). Such a priority has culminated in varied mechanisms and forms of engagement – bilateral and multilateral, formal and informal – in order to influence critical dimensions of cybersecurity in cyberspace, including: human rights, international law and its application, norms of behaviour, Internet governance, the digital economy, cyber capacity building, and development and strategic cyber relations. The Council of the EU has adopted Conclusions on cyber diplomacy (Council of the European Union 2015) that support and indeed affirm the EU's ambitions in this area, in order to address such "cross-cutting and multifaceted issues with a coherent international cyberspace policy that promotes EU political, economic and strategic interests". To this end key *strategic dialogues* on cybersecurity have been established with China, India, Japan, South Korea, and Brazil; the EU has engaged in international platforms such as the London conference with follow-ups in Budapest and Seoul; it has participated in relevant regional and international fora (United Nations Group of Governmental Experts, ITU, Organisation for Economic Cooperation and Development, ICANN, Internet Governance Forum, Council of Europe), as well as enhancing its relationship with other relevant international organisations (NATO) in the development of its Cyber Defence Policy Framework and engaging in capacity building, in particular in the global south. The U.S. has also been a critical strategic partner – the CSSEU asserting that at the "bilateral level, cooperation with the United States is particularly important and will be further developed", notably in the context of the EU-US Working Group on Cyber-Security and Cyber-Crime (European Commission 2013b:15). Indeed, the Working Group was established to tackle new threats in cyberspace, focusing on a) cyber incident management b) public-private partnership c) awareness raising d) cybercrime, out of which was launched the Global Alliance against Child Sexual Abuse Online (European External Action Service 2014). This is not to say that the EU and US are normatively on the same page when it comes all issues related to cybersecurity – the Snowden revelations revealed that they were clearly not when it came to ethical issues related to data access, protection and privacy standards – but that clearly, as with Japan, the EU shared the same normative vision for the Internet in relation to ensuring freedom, access and rights are upheld online. Finally, and of importance here in relation to the Asian context, the EU has also been active in fora such as the Asian Regional Forum (ARF) and ASEAN, were it has sought to support

discussion on cybersecurity confidence building measures (CBMs) (e.g. the EU has sponsored workshops/seminars and co-chairs ARF meetings).

Conclusions

The EU can be conceptualised as an emerging soft power in cybersecurity, with its underlying aim to secure cyberspace through developing mechanisms and cultures of resilience in order to raise preparedness for cyber disruptions and attacks. Indeed, ensuring that the EU and its member states are prepared for and resilient to attacks, sits at the core of the EU's ambition to develop a common culture of cybersecurity internally – and to project this externally. Parallel to this, the EU approach to securing the Internet is driven by a normative agenda that constructs cybersecurity as sound and effective only "if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union" (European Commission 2013b:4). Similar to Japan, the EU believes in an open, free, accessible and democratic Internet space, through which there is respect for the rule of law and the norms that govern cyberspace. Furthermore, as well as developing the EU approach internally through a series of interlocking logics and thus mandates, the EU seeks to engage and project externally an EU model for cybersecurity and internet governance based on the idea of multi-stakeholderism and the principles of mutual responsibility and international (bilateral and multilateral) cooperation.

To this end, the values and foundations of the EU bode well for cooperation in the cybersecurity realm with Japan. They are normatively compatible with regards to their vision of cybersecurity (multi-stakeholder, open, free) – like-minded in the eyes of the EEAS – and thus able to build a positive and trustful relationship through the EU-Japan cyber dialogue – in which to discuss strategic issues of importance to both parties in relation to different aspects of cybersecurity, including cybercrime, critical infrastructure protection and research and development (including through the EU's H2020 programme). The EU is also able to work effectively – in cooperation with Japan – to construct laws and norms, and discuss CBMs for cyberspace in fora such as the UN, ASEAN (and the ARF), the OECD and NATO as well as in follow-up meetings to the London conference on cyberspace. Whilst the Japanese emphasis on deterrence and militarisation implies a more enhanced strategic relationship with the U.S. in the area of cyber defence, its broader strategic interests and vision for security in cyberspace also point to strategic cooperation with like-minded regional organisations such as the EU (and its member states), in order to address what are perceived as common challenges (cybercrime, cyber-espionage, securing the business environment) to ensure that their common normative vision for the Internet and the norms and laws of cyberspace constructed around this (UN Charter, international humanitarian law) are applied, enforced and adhered to globally. With China in particular sitting at the opposite spectrum of this vision – and seen by Japan as the main threat to its cybersecurity (and its broader security) – the EU and Japan clearly have a common incentive to remain and work within the coalition of actors that are working to ensure a secure and open Internet for all, globally.

REFERENCES

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

Bendrath, R., Eriksson, J. and Giacomello, G. 2010. 'From 'cyberterrorism' to 'cyberwar', back and forth: how the United States securitized cyberspace', in J. Eriksson and G. Giacomello (eds) q.v.

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

Brown, I. and Marsden C.T. 2007. 'Co-regulating Internet Security: the London Action Plan'. Available at: http://www.academia.edu/686684/Co-regulating_Internet_security_the_London_Action_Plan (accessed 10 April 2017).

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

Christou, G. (forthcoming 2017), 'The Challenges of Cybercrime Governance in the European Union', *European Politics and Society*, Special Issue, Winter 2017

Christou, G. 2016a. 'The Collective Securitization of Cyberspace in the European Union', draft paper prepared for workshop on *Governing the European Security Space: The EU as an Agent of Collective Securitization Workshop*, Bertinoro, 17-18 October.

Christou, G. 2016b. *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.

Council of the European Union 2016. Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the EU's Foreign and Security Policy. Brussels. Available at: http://europa.eu/globalstrategy/en (accessed 23 March 2017).

Council of the European Union 2015. Council Conclusions on Cyber Diplomacy. 6122/15, Brussels, 11 February. Available at: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf (accessed 23 March 2017).

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. 2014. 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities', *Journal of Science and Engineering Ethics*, DOI: 10.1007/s11948-014-9551-y.

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

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

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.

Eriksson, J. and Giacomello, G. (eds) 2010. *International Relations and Security in the Digital Age,* London and New York: Routledge.

European Commission 2016. Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats, 5 July. Available at: http://europa.eu/rapid/press-release_IP-16-2321_en.htm (accessed February 2017)

European Commission 2015a. European Agenda on Security, 28 April, COM(2015) 185 final. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (accessed 23 February 2017).

European Commission (2015b) A Digital Single Market Strategy for Europe – COM(2015) 192 final. Available at: https://ec.europa.eu/digital-single-market/en/news/digital-single-market-strategy-europe-com2015-192-final (accessed 10 April 2017).

European Commission 2014. European Cybercrime Centre – one year on, Press Release, Brussels, IP/14/129, 10 February. Available at: http://europa.eu/rapid/press-release_IP-14-129_en.htm (accessed 23 March 2017).

European Commission 2013a. Table on the Implementation of the 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', (JOIN(2013)1), Working Document, 28 Feb. Available at: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-strategy-high-level-conference-0 (accessed 24 March 2014).

European Commission 2013b. Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace, Brussels, 7 February, JOIN (2013) 1 FINAL.

European Commission 2011. *European principles and guidelines for Internet resilience and stability*, Version of March 2011. Available at: http://ccpic.mai.gov.ro/docs/guidelines_internet_fin.pdf (accessed 11 March 2017).

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 Commission, DG Connect 2014. EU Cybersecurity Strategy - High Level Conference, 13 January. Available at: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-strategy-high-level-conference-0 (accessed 27 March 2017).

European Commission and European External Action Service (EEAS) 2016. Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats: A European Union response. 6 April, JOIN(2016) 18 final.

European Council General Secretariat 2013. European Council Conclusions, EUCO 217/13, Brussels 20 December. Available at: https://europa.eu/globalstrategy/fr/node/10 (accessed 25 March 2017).

European External Action Service 2014. FACT SHEET: EU-US cooperation on cyber security and cyberspace, 140326/01, Brussels, 26 March. Available at:

http://www.eeas.europa.eu/archives/docs/statements/docs/2014/140326_01_en.pdf (accessed 25 March 2017).

European Union Agency for Network and Information Security (ENISA) 2016. *Definition of Cybersecurity: Gaps and overlaps in standardisation*, v1.0, 1 July. Available at: www.enisa.europa.eu/publications/definition-of-cybersecurity/ (accessed 27 April 2017).

Europol 2014. *European Cybercrime Center (EC3): First Year Report*. Available at: https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report (accessed 24 March 2017).

Kallender, P. and Hughes, W.C. 2016. 'Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace', *Journal of Strategic Studies,* 40(1-2), September.

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

Klimburg, A. and Tiirmaa-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.

Kramer, F.D., Starr, S. and Wentz, L.K. (eds) 2009. *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. 2009. *Cyber Deterrence and Cyber War,* Rand Corporation.

Libicki, M.C. 2007. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press.

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

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

Robinson, N., 2014. 'EU cyber-defence: a work in progress', European Union Institute for Security Studies, Brief No. 10, 14 March. Available at: http://www.iss.europa.eu/publications/detail/article/eu-cyber-defence-a-work-in-progress/ (accessed 20 March 2014).

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 2017).

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

ENDNOTES

[1] Cybersecurity refers to the protection of networks and information systems against human mistakes, natural disasters, technical failures or malicious attacks.

[2] 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 (Klimburg and Tiirmaa-Klaar 2011:8).

[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 connected to it, which does not exist in any physical form' (ISO/IEC 27032, see ENISA 2016).

[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 European Commission, DG Connect 2014.

[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.