PAPER-DRAFT – Please do not cite or circulate without permission from the authors

IPSA/ AISP International Conference 2017

"Political Science in the Digital Age: Mapping Opportunities, Perils and Uncertainties",
4-6 December 2017

Public Private Partnership arrangements for a secure Cyberspace!? The strategic promotion of cooperative partnerships with the cyber security industry & the need for a critical review on the export of digital-surveillance items

Madeleine Myatt, Universität Bielefeld, mandeleine.myatt@uni-bielefeld.de
& Detlef Sack, Universität Bielefeld, detlef.sack@uni-bielefeld.de

1. Introduction

An open, free and secure cyberspace is mainly seen as a key driver for the promotion of political and social inclusion, the diffusion of fundamental rights, economic growth and international competitiveness.[1] In this sense, interconnectivity and the pervasion of digital technologies in the social, political and economic sphere of our daily lives, leads to a constantly growing reliance on the internet and different information and communication technologies (ICTs). As technology - in historical terms – have always been a key driver for change with a transformational impact on societies, the rapid advances in development of ICTs offer new opportunities as well as challenges and risks. Particularly regarding the latter, an increasing demand for secure data transmissions, cloud-services and communication channels can be identified. The shift of more and more public services online, reported security loopholes, hacking-attacks, cyber espionage and a growing public awareness since the Snowden-revelations (The Privacy Surgeon Report 2014) leads to critical voices, emphasizing on the integrity of data and a discourse on technology and data sovereignty (Bendiek 2013). In this sense, cyberspace comes to the fore as a security- relevant area and a matter of national security in a dual perspective: firstly, as a domain of homeland security and public safety in the light of providing security for private users and economic sectors which operate at the blurring line between the real and digital world (e.g. energy, finance, health, transport). Secondly, cyber can be viewed as a providing space, which could become - via the use of digital surveillance items and data-mining tools- a matter of concern. In this context, the influence of digital and smart grid technology as a distinguishing feature of law enforcement and the strategic value of data is visible (e.g. data-mining software, video/audio surveillance, tracking devices, intrusion software, biometrics or IT-forensics).[2]

[1] The Cybersecurity strategy of the European Union: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security . Accessed online: 20/04/2017.

[2] Associated developments regarding homeland security are e.g. addressed in discourse on the concept of "smart policing", see (e.g.): Frois, Catharina; Machadao, Helena (2016): Modernization and Development as a Motor of Polity and Policing. In:

Our digital footprints are in this sense – likewise - a security-relevant resource and an object which need to be protected. In response to the danger and risks of cyberspace, many states take up the challenge by developing and publishing a national cyber security strategy[3] (NCSS), which define their strategic goals, priorities, implementation measures. In some cases, they are complemented by an "action plan". This aspect is also underlined by the OECD comparative analysis of CS-strategies (published in 2012) which refers to the development of a constantly emerging landscape of NCSS-Strategies by subsuming it as a "*new generation*" regarding its priority status and scope (OECD 2012: p.3). Although a first comparative glance at the current NCSS-landscape reveals country and/or regional-specific differences, similarities can be identified. These include a categorization of cyber security as "shared responsibility" with a direct or indirect emphasis on the concept of public private partnerships[4] and a strategic focus on the promotion of the cyber security industry. The latter is often underlined with an intention of becoming or asserting a position as "leading nation"[5] or "forerunner"[6] in cyber security – both – as a strategic signal for preparedness in national security and as competitive advantage in economic terms.[7] This strategic approach finds its expression by accompanied initiatives on the regional and international level. One example is the contractual Public-Private Partnership (cPPP) on cybersecurity between the European Commission and the European Cyber Security Organisation (ECSO), introduced in 2016. Its main objective is to promote the status of the European Union as an independent security actor by "*building a strong, resilient and globally competitive European cybersecurity industry with strong European-based offering*".[8] While the majority of previous research in the field of cyber security focus on public private partnerships with regard to the protection of critical infrastructures, the project stays abreast of changes and put a special emphasize on a comparative analytical view on launched partnerships

Ben Bradford, Beatrice Jauregui, Ian Loader und Jonny Steinberg (Hg.): The Sage handbook of global policing. Los Angeles, London, New Delhi, Singapore, Washington, DC, Melbourne: Sage reference, 391 ff. (412–420).

[3] See NATO CCDCOE: https://ccdcoe.org/cyber-security-strategy-documents.html and e.g.:
Sabillon, Regner; Cavaller, Victor; Cano, Jeimy (2016): National Cyber Security Strategies: Global Trends in Cyberspace. In: International Journal of Computer Science and Computer Engineering, Vol.5 (5), pp. 67-81.

[4] Carr, Madeline (2016): Public-Private Partnerships in national cyber-security strategies. In: *International Affairs* 92 (1), S. 43–62. See (e.g.): Linder, Stephen H. (1999): Coming to Terms with the Public-Private Partnership. In: *American Behavioral Scientist* 43 (1), S. 35–51.; Oppen, Maria; Sack, Detlef (2008): Governance und Performanz. Motive, Formen und Effekte lokaler Public Private Partnerships. In: Gunnar Folke Schuppert und Michael Zürn (Hg.): Governance in einer sich wandelnden Welt 41/2008. Wiesbaden: VS Verlag für Sozialwissenschaften / GWV Fachverlage GmbH Wiesbaden. Verma, Manisha (2016): Role of State in Partnerships with the Private Sector. In: *Journal of Development Policy and Practice* I (1), S. 53–70.

[5] See for example: NCSS India.

[6] HM Government United Kingdom (Hg.) (2016): National Cyber Security Strategy 2016-2021. London, United Kingdom.

[7] For instance expressed by the Chancellor of the Exchequer Philip Hammond MP (UK), who pointed out: "Partnerships with industry and academia, will allow us to take even greater steps to defend ourselves in cyberspace and to strike back when we are attacked." See: https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy (access on 23/04/2017).

[8] For more Information see: https://ec.europa.eu/digital-single-market/en/cybersecurity-industry (access on 25/11/2017)

arrangements between the public sector, the cyber security industry and science (including a reflection of the intended role of civil society). It does so by taking into account that cyber security appears in practice as an umbrella concept which links different policy fields i.e. security, international affairs, economics, technology and science. With this in mind, our paper deals in particular with hybrid organisational arrangements in the field of cyber security and the question which main drivers explain particular "collaborative governance" (Ansell/Gash 2007; O'Leary/Vij 2012) and "shared responsibility". In examining this question our argumentation contributes to the characterisation of cyberrelations by highlighting a specific mode of organisation. On that basis we can expose the (reputed) role of public private partnership arrangements as strategic tool in power politics and relations in cyberspace.

We will close our argumentation by giving a first glance on the export dimension of cyber security technology as a consequence of the strategic approach of becoming a 'forerunner' or 'leading nation'. This outlook offers the possibility to link the discussion of PPP as strategic tool in the field of cyber security to the controversial debate regarding the export of "dual-use" digital surveillance technologies and a possible abuse by autocracies and/ or hybrid regime.[9]

2. Literature review and assumptions - Cyber security and PPP state of the art

2.1 Defining Cyberspace and cyber security

Because there is neither a consistent nor clear definition of the two basic terms which frame our argumentation, preliminary remarks have to be made regarding a terminological and conceptual clarification.

Cyberspace

As the conceptualisation of cyber security refers to cyberspace as a subject matter for providing security and moreover shapes the perspective on the question, how to govern and regulate cyberspace, the definition of the term will be prefixed. In terms of getting closer to the conceptual fundament, a variety of definitions come to the foreground.[10] Correspondingly, national and international entities as well as different technical bodies offer quite different concepts regarding the scope of descriptive characteristics. Beside all differences, similar ideas of interconnectivity and virtuality are present.

[9] In this context the Wassenaar Arrangement (http://www.wassenaar.org/) serves as a central point of reference and also the identified need for action by the European Union in September 2016 (see Press Release by the European Commission (28/09/2016): http://europa.eu/rapid/press-release_IP-16-3190_en.htm)

[10] See e.g.: NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/cyber-definitions.html , last access: 12/11/2017.

Therefore, cyberspace can be defined - in a simple and short manner - as a shared global medium and infrastructure for communication as well as data or information exchange (e.g. Cornish 2015). This includes interaction between machines (e.g. all kinds of ICT-products, incl. the internet) and humans, but also machine to machine communications. By taking the respective role of humans into account, the definition which is going to be used here, is in line with the so called "cybernetic perspective" which captures cyberspace as a *"metaphysical construct created from the confluence of digital hardware, the data it creates and manages, and the human that interact with the hardware"* (Edgar/Manz 2017: p.35).

This rather large-scale definition is not just reduced to a focus on data/ information and the technical infrastructure that enables exchange and transmission. It already refers to recent developments, subsumed under the phrase "**I**nternet **o**f **T**hings" (IoT) and its extension to the "**I**nternet **o**f **E**verything" (IoE), which moves from maschine-2-maschine communications to the description of a more complex system, which takes humans and processes into account. In this context, it is important to emphasis, that these two phrases and linked concepts are to a high extend shaped and distributed by private actors. This reference is being made consciously, to point to the reciprocity of different actors in terms of the construction of conceptual meaning and interpretation attempts. The presented perspective indicates, that cyber as a space concept includes not a physical environment, but covers a perception as virtual.[11] It is moreover a virtual interaction space, created by humans and not just a neutral operating system. This view has an impact, especially with regard to the disseminated perception that cyberspace incorporates a parallel existence of challenges and opportunities and is furthermore marked by competition and collaboration. Especially regarding the first, humans in general show the tendency – as Paul Cornish states – "*to ensure*" [that the inherent interrelation between challenges/risk and opportunities] "*is defined more by opportunity than by challenge*" [and therefore] "*the human instinct is to oversee and to regulate"* (Cornish 2015: p.15). Regulation can of course appear in different forms and is linked to different ideas. This remark is not a trivial notion with view to the concept of cyberspace in terms of its internal relations and governance approach. So, the question is, in which direction the idea of cyberspace is further developed with regard to a regulation attempt? Is it seen as a hierarchical organized global management system, a self-regulated network or as a key driver for the promotion of political and social inclusion, human rights and emancipation which requires the establishment of a comprehensive and common regulatory framework (Cornish 2015). These three directions of impact influence further aspects like actor constellations, the role of state sovereignty, data sovereignty and the

[11] Blurring lines to the physical world are taking into account, especially in matters of security.

regulation scope and shape and the linked concept of cyber security. The collision of these different views can already be observed in international politics of cyberspace with regard to controversies between western states and China or Russia. Moreover, the different perspectives effect the idea of engaging and building partnerships with private actors and the differences in their manifestations. Therefore, our argumentation puts light on cyberspace as an interaction field between different actors by referring to the observation - based on a comparative analysis of NCSS - that Public Private Partnerships arrangements appear as a mode of organisation in cyber security relations and puts emphasis on the defence and security relevance of cyberspace.

Cyber security

> "Cyber security is a shared responsibility of all government entities, businesses, institutions, and individuals (…)" (NCSS-Qatar 2014: vii)

The question what cyber security is or should be, is a subject of an even larger and ongoing debate in academia, marked by its permanent evolving nature in terms of a high frequency of innovation. In respect of both – threats and risks as well as defence and deterrence. With view to the NCSS-landscape the conceptual scope and idea of cyber security is often linked to a specific idea and understanding of society in the digital age, like a categorisation as information society (e.g. Finland). For that reason, our argumentation is based on a broad definition of cyber security which captures all kinds of measures and actions which are taken to protect information/data, communications and technology from damage, caused by accident (technical & human cause), natural incidents or purpose (e.g. Guiora 2017: pp.15-20). To be more precise, this includes all measures which are established to prevent, deter and detect unauthorized access, theft, the manipulation and destruction of data, infrastructure, technology and communication/ information traffic (Edgar/Manz 2017: pp.36-37, e.g. NCSS-UK 2016). Correspondingly, cyber security includes technological solutions and innovations, policies and procedures which explicitly address efforts for a secure cyberspace. These can also operate at the blurring line between cyberspace and the "real" World. Here, the idea of cyber security as umbrella concept comes into play. In sum, cyber security is a more inclusive term than related concepts like internet or network security. With view to the CSS-Landscape three core attributes are dominant in terms of a goal formulation: (1) the preservation of **c**onfidentiality, (2) **i**ntegrity of information/data, (3) **a**vailability (e.g. UN, NCSS Sweden), sometimes subsumed under the acronym CIA. To pursue these strategic goals, collaborative action is mainly seen as the key driver to pursue and achieve the common goal -cyber security. This argumentation is based on a definition of cyber security as '*shared responsibility*' which is present in various NCSS. As the German NCSS (engl. Version) quotes:

'*Ensuring cyber security, enforcing rights and protecting critical information infrastructures require major efforts […] Given the shared responsibilities of the state, the industry and society a cyber security strategy will only be successful, if all players act as partners […]*' (NCSS Germany 2011: p.4)

To extend this illustration, the English counterpart claims that the Government will *'[…], working together collaboratively with industry and academia [to] define what cyber security looks like.´* The latter also serves as an example for the role partnership arrangements as discourse arena. In sum, the question can be raised which collaborative arrangements and mechanism can be brought into play?

2.2 Definition of Collaborative Governance (CG)

Referring to the (alleged) mode of organisation in the field of cyber security the following paragraphs address the likelihood of calling for PPP in CS as well as establishing them. In the following the context of the mode of organization is displayed. PPP in Cs are by definition a case of "collaborative governance" (Gash 2016) which can be broadly defined in the following sense: "*Collaborative public management is a concept that describes the process of facilitating and operating in multi-organizational arrangements to solve problems that cannot be solved or easily solved by single organizations"*. Collaborative means to co-labor, to achieve common goals, often working across boundaries and in multi-sector and multi-actor relationships. Collaboration is based on the value of reciprocity and can include the public." (Agranoff/McGuire 2003)

<u>Characteristic features of CG include:</u>

The general appreciation that individual action might be insufficient for a rather broad range of reasons (individual lack of money, assets or knowledge etc.) results in some kind of joint action of organisations. The constraints of acting alone trigger co-operation.

Depending on the good to be produced the logics, programs and capabilities of one societal sub-sector might be insufficient. For instance, security as a collective good can (depending on the resources of a particular sub-system) be produced only by the state (non-collaboration) or by the state and private actors coming from science or economy. CG covers (continuous or discontinuous) relations between actors from different societal sub-systems such as politics, economy, science to name but a few. *Functional differentiation* is the pre-condition of CG. Actors from different societal sub-systems lack the capabilities and resources to act on them in order to produce a particular (collective) good.

In this regard, PPP is a rather general label addressing collaboration across different domains and sectors. PPP entails (still in a rather broad sense) communication and interactions of actors which rationalities and programs (i.e. not their interests) differ notably. The *cross-sector interaction* is based on both the need to combine differently allocated resources and the gain of knowledge extracted from different sub-systems.

Collaborative governance includes *joint operation*. Different from coordination of individual actions of its constituents, co-operation and collaboration address some form of continuous joint interaction be it in an organization with mixed-ownership, be it in relations based on incomplete contracts.

CG includes the *concerted allocation of resources* (finance, assets, knowledge) *and risks*. (Contractual) stipulations of the allocation couple the networks. The stipulations establish the respective tasks, contributions, and gains. Since the actors stem from different social sub-systems joint agreements and contracts are subject to different interpretations, misunderstandings and self-serving appreciation. Therewith, the readiness for re-negotiate, the competence to tackle cognitive dissonances, and interpersonal trust are to be deemed as necessary capabilities of the actors involved. Because of the impossibility of stipulating all details of resources allocation, changing environments, and basically different perceptions PPP are rather dynamic organizational entities (Kouwenhoven 1993; Ansell/Gash 2007; O'Leary/Vij 2012; Gash 2016).

Therewith, collaborative governance and PPP in general are based on a couple of conditions (functional differentiation, lack of resources for collective goods, acknowledgement of fundamentally different logics and programmes, stipulated allocation of resources and risks, flexible management of organizational dynamics) which makes joint action a project with a rather number of prerequisites. In considering CS as a notable sensitive collective good, CG and PPP are not likely to be implemented. At least, it needs to be discussed which contextual factors convey and trigger PPP in this area. In order to debate the likelihood of CG in this area we shed light on the politico-economic context of the different states.

2.3 Politico-economic context of PPP in CS

Varieties of capitalism

As PPP in CS couple the economic and political societal sub-sector, we address the debate on "varieties of capitalism" (Hall/Soskice 2001). By turning to this debate, we elaborate on the institutional tradition of the state-market relations in a country. We assume that the general "path dependency" of public-private relations in a country impact on the likelihood on CG in

the field of CS (Pierson 2004). We argue that both a general 'climate' for cross-sectoral co-operation as well the experience of administration and firms with collaboration with actual collaboration in the past have an effect on the readiness for setting-up PPP in CS. The debate (Amable 2003; Hancké 2007; Gualmini/Schmidt 2013; Nölke et al 2014) identified four patterns of state-market relationship in developed capitalist states:

1. The liberal market economy (LME) mainly of the Anglo-Saxon states is based on a weak tradition of state-market interaction and a high degree of competition between firms. The production of collective good is rather weak in general and based on contractual relationships if it occurs. However, these states experience a rather encompassing debate on PPP since the 1990ies. This is valid for UK on particular.
2. The Japanese model rests on innovations and production of public goods which are triggered mainly within large TNC with a rather high regulatory independence from state. Nonetheless, personal networks penetrate market and state. Market activities are coordinated within the big Japanese conglomerates.
3. The coordinated market economy (CME) with its long tradition of dense state-market relations involving not only conglomerates but also SMEs constitutes a next tradition and institutional pattern. Production of collective goods is based on a strong role of firms in dense interaction with the state.
4. The "state-permeated market economy" needs to be understood as being based on state-market relations in which the state and politics are pre-dominant. These states show a strong tradition of state's intervention in the economy and neo-mercantilist policies in which the firms are sub-ordinated to the 'planification' of the state. France and China are, despite their different political systems, typical examples of these states.

Against this background, we consider the traditional institutional patterns of state-market relations with a pre-dominance of either the market (pattern 1) or the state (pattern 4) the less likely for PPP in CS and the idea of "shared responsibility". Continuous and institutionalized dense state-market relations (pattern 3 in particular) are rather prone to CG in this field because of a tradition of both cross-sectoral resource dissemination and experience with joint action.

H 1: Due to path dependencies and the tradition of state market collaboration CME are more likely to set up PPP in CS than LMEs.

Concentration of executive power in political systems

The institutional patterns of the political system itself (Tsebelis 2005; Lijphart 2012) are also likely to influence the readiness for PPP in CS. A strong role of the state in the production of public goods is based on its organizational capabilities and the degree of horizontal as well as vertical concentration of its resources. As long as the state is capable of allocating all resources necessary for production of collective goods on its own, its willingness to address other actors, in particular actors from different societal sub-systems, remains low as no need is to be seen. This is true for the field of security in particular as it is seen as the pivotal task of the state and its 'raison d'être'. Thus, we assume that the concentration of state power on the executive (i.e. government) reduce the willingness of the state addressing other actors (i.e. firms) due to its capabilities to act on its own. In reverse, it is likely that the spread of (horizontal as well as vertical) executive power and a high number of institutional veto-players increase the readiness for CG. This assumption derives from two arguments. As already mentioned, the insufficient resource allocation might require the pooling of resources of other actors. This is the argument of scarcity. In addition, political systems with a high number of veto players stimulate cross-sectoral co-operation to overcome stalemates by decision-making outside the political system. This is the argument of institutional circumvention. Effectively, we assume that a consensus democracy is in general more willing to engage in CG due to the both reasons given.

H2: Consensus democracies with a high number of institutional veto players are more likely to establish PPP than democracies with a concentrated executive power.

Tradition of public procurement

In effect of both mode of capitalism and concentration of executive power, states differentiate in their share of buying in public services from firms. The inclination for contractual PPP is indicated by the share of public procurement in a country. The tradition of contracting-out (instead of in-house production with the public administration) can be displayed by the share of public procurement of the GDP (percentage) and of the government's expenditures. Data show (OECD 2015: 137) notable differences as some states (The Netherlands, Korea) spent over 40 % of their total expenditures on public procurement while other countries' share (for instance Switzerland, Spain, and Ireland) is below 25%. As the share of public procurement indicates a tradition and practice of contracting-out we assume the following:

H3: States with a high share of public procurement are more likely to establish PPP than those with a low share.

Tradition of law and order politics

Focusing of the institutional traditions as the context triggering PPP in CS, we turn to the policy subsystems in question. It remains to be controlled, if the rather general assumptions for the varieties of capitalism and political systems match with the area in question. This area is composed by both the institutional patterns shaping law and order politics and the ICT affinity in a state. Addressing law and order policies as an organisational field with a particular purpose (security), different pattern are to be identified in international comparison (Wenzelburger 2014; 2015). In taking state's expenditures in the field, the rate of prisoners, and the personnel into account, one can distinguish different clusters in the OECD-'world'. The main distinction is between the Scandinavian states with a rather low level of state's expenditures, prisoner's rate, and personnel vs. the 'punishing' Anglo-Saxon states (UK, USA) with the reverse parameter values. Applied to Cyber Security strategies, we suppose the issue (security) is rather high on the political agenda in the (Anglo-Saxon) states with a rather outstanding tradition of securitisation. This is likely to result in quick and rather broad activities in the field. Since the rate of personnel is high we suggest firstly – in line with the argument on the concentration of executive power (see above) – that the 'punishing' states neither have the need for CG nor are they willing to diminish their capabilities by bringing other actors in. Secondly, it is also known that both states have a strong tradition of privatizing tasks in the field via contracting-out (Garland 2007) which then lead to a modification of the argument.

H4: States in which security issues are high on the political agenda and which display a strong tradition of contracting-out in the field are more likely to establish PPP in CS than states with low resources and prisoner's rates.

Tradition of defence policies and foreign affairs

The likelihood and capabilities for active CS strategies derives from the perceived threats in international relations and the state's own geo-political needs and strategies. Even if geo-political strategies are based on much more complex patterns of interaction in foreign affairs the governments' expenditure on the issue indicate the relevance of foreign affairs. States like

Israel, United States, and Korea spent notable more than the mean of the OECD states. Austria, Ireland, and Hungary are among those states with a very low share.

H5: States with a high share of expenditures in defence (i.e. geopolitical activity) are more likely to set up a proactive CS strategy.

IT-affinity

CS is not only about security, home and justice affairs etc., it is about digitalization, a particular vulnerability (critical infrastructures) that goes along with digital penetration, and, therewith, with a particular level of IT-affinity. Affinity is understood as digital penetration of the economy, administration, and social living which goes along with both a particular capability in IT and a notable susceptibility to cyber attacks as these display a deeper impact than in states with a rather low level of IT penetration (Baller et al. 2016). In general, we assume that the states with a rather high level of IT affinity are prone to state's activity in the field.

H5: States with a high IT-affinity are more likely to set up an active CS strategy.

In order to consider the inclination of states setting up PPP in CS one might take into account a simple calculation. As governments are only willing to launch CG as a cost-intensive activity if they benefit from the resources of the private sector the capacities of the IT firms are of particular importance. The innovativeness of IT business can be measured by the patents application in the field (Baller et al. 2016: 248). Putting it negatively: As long as firms do not contribute to a PPP with crucial resources (IT knowledge), there is no need to include them in co-operation. In this regard, Japan, Sweden, Switzerland, Finland, and Israel display a rather innovative private IT sector while some other states with a rather high IT affinity in general show low innovative IT skills in private firms.

H6: States with an innovative private IT-sector are more likely to set up a PPP in CS.

Public Procurement in IT

Similar to a contracting-out tradition in home and justice affairs, the inclination of governments for purchasing technology products differs notably (seeing Qatar, United Arab Emirates, Malaysia, and Singapore at the top of the list). Apparently, states make different decisions on

buying-in sensitive IT products. We assume that a state with a high share of public procurement in this area is more willing to rely on CG due to the experience with firms.

H7: States with a high share of contracting-out of technology products are more likely to establish PPP than those with a low share.

3. Cyber Security as "shared responsibility" – An empirical insight in the relationship between public & private actors

With view to widespread reference on CS as "shared responsibility" the direct or indirect linke to the concept of public private partnerships (PPP) refers to the progressive digitalisation of the political, economic and social sphere by stressing on a corresponding need for technology innovations which provide security, ensure privacy and foster liability.

The evolving and transnational nature of cyber threats and risk serve as a trend booster and make PPP forms an appealing solution. Private actors provide infrastructures, hard- & software supply, they offer services and updates on a broad scale and for multiple purposes. In this sense, they offer relevant technology solutions and knowledge, e.g. in terms of hazard identification, security loopholes, incidents, threat scenarios as well as defence solutions and strategies. On this occasion, the first public/ private relation or partnership based action, which should be addressed, is the hackback-strategy of private companies. They have recently gained public attention as a subject of controversial debates which lay focus on the questions: If hackbacks can serve as a contributing element of cyber defence and which role private actors can or must play in cyber security?[12] A prime example is the Microsoft case which serves as a point of reference in literature (Hiller 2014). Microsoft used a strategic combination of legal action and the development of technical tools to strip down botnets[13] and stop their proliferation (Hiller 2014: pp.177-184, see also Bendiek 2016: p.26).

The adopted strategy was incorporated in an argumentation line which put emphasise on addressing a security problem of global scale by using proactive action. The strategical continuation is moreover visible in their recent court success (U.S. District Court, Eastern District of Western Virginia) against the Russian hacker group 'Fancy Bear(s)' in August 2017 which also permits proactive action in form of taking over the servers in use.[14] With view to

[12] Just to mention one example, the German Government discussed the so called "Hackback-Strategy" with view to the principle of a 'militant or well-fortified democracy' in line with the German Basic Law in April 2017. See: https://www.heise.de/newsticker/meldung/Cyberschlaege-Bundesregierung-prueft-Hack-Back-Strategie-mit-digitalem-Rettungsschuss-3689279.html (access on 25/11/2017).

[13] A botnet is a network of automatized malware (Bots) which infect computers via an authorized code and network connections.

[14] See e.g.: https://www.digitaltrends.com/computing/microsoft-fancy-bear-russian-hackers/ (access on 25/11/2017).

the current NCSS landscape, the cyber security industry sector is more and more addressed as a key point of reference. It serves basically two major needs: (1) a necessary contribution in terms of providing security and a secure digital infrastructure and (2) the offering of promising and profitable industrial sector. The latest cyber security market report published by Cybersecurity Ventures in May 2017 values the global cyber security market to be worth round about 120 billion US dollars and predicts an annual market growth between 12 and 15 per cent through 2021 (alternative resources from 2015 set the annual market growth between 8-10%).[15] Besides, the annual market growth, a dominance of global suppliers (e.g. Microsoft, Cisco, IBM) based in North American for software and the Asian-Pacific Area for hardware is visible (ECS cPPP Industrial Proposal 2016: p. 16). For that reason, European actors emphasis on homegrown innovation and capacity developments to reduce interdependencies and strengthen the own regional position (ECS cPPP Industry Proposal 2016: p.12-13). Similar argumentation can be observed on the national level and with view to the NCSS landscape (e.g. UK, India, Finland). Government bodies and public actors impersonate as costumers (e.g. public services, e-Government) but also specifically in the course of their mandate for action regarding the provision of safety and security. Both, with the civil society in multiple ways. In an attempt to capture and characterize the relation structures of cyberspace – moreover in the field of cyber security - the close reciprocity of public and private actors in the domain of security is a distinguished feature. As the National Cyber Security Centre of the Dutch Ministry of Security and Justice quotes:

> *"Public private partnerships are essential to NCSC because it needs intensive cooperation to maintain a robust resilience of the Netherlands against cyber security threats."*[16]

This raises the question, which organisational and conceptual ideas of PPP is linked to the strategic goal-setting in CSS are visible in practice. A comparative perspective points at two models which appear recurrently in the field of cyber security. First, the establishment of information-sharing and capacity building formats and second, contractual based public private partnerships. Although the spread of the basic formats makes a common pattern, differences can be identified with view to their specific implementation. The latter is linked to the particular politico-economic and security cultural context, as we already argued in the previous section. Referring to the first model the following examples illustrate the spread and variety of country specific implementations. Finland's defined PPP in cyber security is the National Emergency

[15] See: https://cybersecurityventures.com/cybersecurity-market-report/ (access on 27/11/2017).
[16] See: https://www.ncsc.nl/english/Cooperation/public-private-partnership.html (access on: 25/11/2017).

Supply Organisation (NESO)[17] which is basically a network of various public-private partnership initiatives, related to the security of supply. Germany developed a similar framework but based on a broader scope. The '*Allianz für Cybersicherheit'* (ACS)[18] serves as a cooperation platform founded by the Federal Office of Information Security and Bitkom (Germany's digital association). The ACS also offers services like short audits of cyber security capacity and threat analysis. The United Kingdom as presenter of the Anglo-Saxon model implemented: (1) Cyber Security Information Sharing Partnership (CiSP), a joint industry and government initiative to set up the exchange of cyber threat information (RUSI 2016), (2) Cyber Growth Partnership (CGP) which brings together "*representatives from UK industry, government and academia; working in partnership to promote and create opportunities for UK cyber security companies*"[19]. Moreover, the UK government takes on the role as agent and extend their range of offered services by fostering export opportunities on cyber security.[20] The last two aspects are in line with attempts to occupy a position as leading nation, underpinned by a "strong" cyber security industry. Furthermore, the UK can look back on a rather long history of PPPs in the field of public safety, including the use of digital surveillance technologies. Entirely in line with our remarks on VoC, the case of the United States follows a similar path as the UK and shows a strong tendency for public private partnership arrangement in various forms, predominantly in subfields like generating public awareness, combating cybercrime (international scope), solving software and hardware vulnerabilities (e.g. zero-dates exploits) including securing e-government services, attributing cyber intrusions to state-sponsored attackers as well as securing private systems (Busch/Givens 2012,p.4 see also: Eichensehr 2016, p.478-499). The National Cybersecurity Alliance (NCSA) which promotes awareness raising for cyber security issues and the contractual PPP with Microsoft Cloud for Government are just two examples for the range of implemented PPP forms in U.S.[21] As Kristen Eichensehr emphasised, '*academic literature and public debate have not fully appreciated the extent to which the United States has already backed into a de facto system of "public-private cybersecurity"'* (Eichensehr 2016: p. 470). The big global players like Microsoft, IBM or CISCO offer an increasing manner of cyber security or security services via cyberspace for

[17] For more information see: https://www.nesa.fi/organisation/the-national-emergency-supply-agency/ (access on 26/11/2017)
[18] For more information see: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html (access on 26/11/2017)
[19] More information on CGP: https://www.gov.uk/government/collections/cyber-security-export-help (access on 27/11/2017)
[20] See: https://opportunities.export.great.gov.uk/opportunities?utf8=%E2%9C%93&isSearchAndFilter=true&filterOpen=false&s=CYBER+SECURITY&commit=Find+opportunities (access on 27/11/2017)
[21] See: https://enterprise.microsoft.com/en-us/trends/the-microsoft-cloud-for-government/ (access on 28/11/2017)

governments.[22] The Microsoft Digital Crime Unit is just one example. One of its key elements is an innovative PhotoDNA tool, developed in cooperation with science, namely the Dartmouth College and praised as an important partnership for global law enforcement. It basically creates '*a unique, fingerprint- like signature for digital images*' which can be used to trace them down in cyberspace.[23] This tool is already been used by companies like Facebook or Twitter to scan their services and identify child pornography or other images of criminal relevance. On that ground partnership-based action evolves and are intended, which includes law enforcement. Moreover, the tool was also donated to the U.S. non-profit cooperation, the National Centre for Missing & Exploited Children.[24] This move integrates partnership relations on a broader scope, by involving civil society which simultaneously serves to strengthen and create a respectively role image. Another example which illustrates the amount and distribution of PPP in the Asian-Pacific Area Transparency and Cybersecurity Centre launched by Microsoft in Singapore in October 2016.

The example of Japan illustrates an orientation towards purchasing expertise and advanced cyber security solutions based on transnational market relations (incl. transnational business to business and business to government relations). Therefore, Japan developed and maintains a close relationship to Israel (one of the major CS exporter) and Israeli cyber security companies. In this context, it is important to note, that many Israeli cyber security companies have military background with view to their personnel structure. Both governments announced a joint collaboration in May 2017 which serves as the fundament for a "*cooperation between Israeli governmental bodies, economic organizations and companies with Japanese companies in a variety of fields*".[25] On that occasion collaborations in cyber security is integrated as a major element and set out in a memorandum.[26]

3.1 Public Private Partnership arrangements for a strong cyber security industry

PPPs in their different appearances serve in the field of cyber security as an organisation mode which pursue the goal, to set a visible interactions frame for public and private actors, bridge information asymmetries and gain competitive advantages. With view to the latter and in

[22] PPPs und CS Products by Microsoft are just integrated as examples. Other global player and also SMEs offer similar products or are involved in similar PPP-arrangements.
[23] Microsoft Story Laps Section: Digital Detectives: https://news.microsoft.com/stories/cybercrime/index.html (access on 28/11/2017).
[24] See: National Center for Missing & Exploited Children : http://www.missingkids.com/footer/aboutus (access on 28/11/2017).
[25] For more details see: http://mfa.gov.il/MFA/InnovativeIsrael/Economy/Pages/Israel-and-Japan-launch-new-cyber-security-collaboration-11-May-2017.aspx (access on 27/11/2017).
[26] The memorandum is available online at: http://www.meti.go.jp/press/2017/05/20170508004/20170508004-5.pdf (access on 27/11/2017).

recourse to the sketched PPP implementations, the relevance of partnerships with the cyber security industry and science comes to the fore. It merges moreover with attempts of industry fostering to gain economic and power advantages. A prime example with view to our remarks on the political-economic context and our hypotheses, presents the NCSS UK which put a special emphasize on the central role of an innovative cyber security industry and links the promotion of collaboration between the private sector, science and public actors as fundamental for assert a world-leading position.

> '*The Government will support the creation of a growing, innovative and thriving cyber security sector in the UK in order to create an ecosystem where:[1] security companies prosper, and [2] get the invest they need to grow, the best minds from government, academia and the private sector collaborate closely* […]' (NCSS UK 2016: p. 57).

Moreover, the UK case can be seen as representor for NCCSs which include a proactive orientation, as they include respective technology like digital surveillance. Especially, with view to a cyber conflict scenario with "foreign actors" the UK version states:

> *'Our investment in sovereign capabilities and partnerships with industry and the private sector will continue to underpin our ability to detect, observe and identify […].' (NCSS UK 2016: p.49).*

The Fostering of partnership arrangements between public actors, the cyber security industry and science can also be found on the regional level. The contractual Public-Private Partnership (cPPP) on cybersecurity between the European Commission and the European Cyber Security Organisation (ECSO) which has been introduced in 2016 serves as forerunner on this occasion. Its main objective is to promote the status of the European Union as an independent security actor by "*building a strong, resilient and globally competitive European cybersecurity industry with strong European-based offering*". A Similar attempt can be observed in case of the ASEAN. In 2016, member states called for a tighter cyber security coordination[27] and launched Cyber Capacity Programme (ACCP) in April 2017. In sum, a strong cyber security industry serves more and more as strategic value and fundamental element. This is not remarkable, if cyber security is defined as an umbrella concept of various policy areas. But also, the identified market size and growth rates play an important role and can develop a corresponding dynamic.

[27] See: https://www.csa.gov.sg/news/press-releases/asean-member-states-call-for-tighter-cybersecurity-coordination-in-asean (access on 28/11/2017)

Market Size and Growth for network and information security products (classified as "civilian")

Market Breakdown by Solution/ Services	**2014** € bin	Market %	Average growth in the next 10 years
Governance, vulnerability and cybersecurity management	2,7	4%	11%
Identity and access management	7,3	11%	10%
Data security	11,3	17%	6%
Cloud security	2,7	4%	12%
Applications security	2,7	4%	7%
Network systems security	14,7	22%	5%
Hardware security (device/endpoint)	4,0	6%	6%
Audit, planning and advisory services	9,3	14%	6%
Management and operation services	2,0	3%	7%
Managed security services (MSS)	9,3	14%	15%
Security training services	0,7	1%	10%
TOTAL	**66,7**	**100%**	**Higher than 8%**

Source: ECS European Cybersecurity cPPP – Industry Proposal (2016), p.22

This overview and especially the rather broad product categories have to be complemented by further explanations. On this occasion, it seems to be reasonable to add or rather list data & predictive analytics, forensics, biometrics and all other kind of intelligence based cyber solutions (e.g. intrusion software) in a sub cyber security market segment. The latter can be illustrated by taking the intel Market report from 2013 into account, which attest the industry of Digital security and surveillance (DSS) a market value of 40 billion US Dollars and a compound annual growth rate of 9–12 percent.[28] In sum, a strong cyber security industry serves not only as competitive advantage in security but also in economic terms. Here, PPP arrangements seem to play a predominant role as mode of organisation in international relations and world politics.

Two further observations at least support these implications. First, the following pattern can be observed in well-known discourse arenas of international security relations (e.g. the Munich or

[28] See intel Market overview: Powering your DSS Designs, available online at: https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/dss-market-overview.pdf (access on 28/11/2017).

Berlin Security conference): The integration of either specific industrial cooperation panels or high- level debate formats with a public private line-up speaks for itself. Second, the distribution of country or regional reports by i.e. PricewaterhouseCoopers International (PwC) and similar consulting networks, companies and think tanks which focus on the respective cyber security market potential, illustrate the dynamic relation between the market dimension and security relevance. Moreover, if it is taking into account, that these reports serve as reference source for government officials and are also used in the context of at least some NCSS (e.g: NCSS UK 2016).

4. Outlook: The attempt of becoming a "leading nation" in cyber security & its downsides

Having displayed the PPP as a prominent if not prevailing mode of organization further research is dedicated to the particular risk allocation in CS PPP.

As the idea of a strategic value of an effective cyber-industry via PPPs comes to the forefront and also shape cyber relations, the development of digital surveillance items (as part of the cyber product range) respectively underlines the 'forerunner' or 'leading nation' attempt. For that reason, the pervasion of digital surveillance technology which addresses the strategic value of data, includes challenges. Moreover, it addresses the question, if technologies of security can turn into technologies of insecurity in the national context as well as world politic relations. Therefore, the export dimension of digital surveillance items and especially so called "dual-use" goods needs to be addressed in further research.

The International trade of surveillance technology is not a new matter of concern (Morton et al 2004, see also: Lyon 2006), although their further development in the digital age includes remarkable range-extending abilities. After the end of the Cold War, the use and development of new surveillance technologies expanded to law-enforcement and the private sector (Wright/ STOA Report 1998: p.15). The reason for the latter is a strategic reorientation including effects on the government funding focus. The outlined developments caused a dynamic in a twofold manner: First, the defence industry penetrated in the field of CS to compensate cut-downs and second, civil ICT companies enter the scene as competitors in that field (see also: Bendiek 2016: p.27).

For that reason and due to the strategic value of some digital surveillance items and their implications for human rights, it is important, to take the regulatory mechanisms and existing trade control regimes into account which focus on so called 'dual-use' goods. According to the EU definition this category includes '*goods, software and technology that can be used for both*

civilian and military applications and/or can contribute to the proliferation of Weapons of Mass Destruction (WMD)'[29]. Especially with view to the trinity of national frameworks, the Wassenaar Arrangement and the EU (Alavi/Khamichonack 2017, Herr/Rosenzweig 2016) further research demand can be identified due to a review and discourse on further needs of regulation as well as a modernisation and enlargement of these control regimes. Important suggestions have been made by human rights organisations like Privacy International (Privacy International Report 2016) and the EU (EPRS Briefing Paper & EC Press Release 28/09/2016).[30]

5. Closing Remarks

In summary, PPP in CS pose a particular problem of modes of organization in international relation and world politics: In one PPP a risk allocation needs to be settled which deals with the logic of conflict and building alliance between states on the hand. These intergovernmental dynamics enable and constraint agency in the PPP. They also trigger particular technological innovation as well property rights. On the other hand, the business community involved in collaborative governance is embedded in a rather different environment which consists of completion and co-operation in a transnational military and civil market. Business involved will be rather reluctant addressing needs and challenges deriving from intergovernmental dynamics as they need to organise their profit and organization survival. Problems arising are for instance the flow of knowledge and innovation from PPP with a particular nation state in a multinational corporate group which addresses 'foreign' governments as customers. In turn, the corporations are confronted with a political environment in which attacks, unrests, and wars as well as the split up of old and the establishment of new alliances result in turbulent markets. How PPP in CS tackle these problems in order to perform and fulfil the task is a matter of future research.

[29] See European Commission (Import & Export Rules): http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/ (access on 28/11/2017).

[30] The process and negotiations on this account have not been completed in 2017 (See also: SIPRI Report 2017).

References

Aas, Katja Franko; Gundhus, Helene Oppen; Lomell, Heidi Mork (2009). *Technologies of insecurity. The surveillance of everyday life.* London: Routledge-Cavendish.

Agranoff, Robert and McGuire, Michael (2003). *Collaborative Public Management: New Strategies for Local Government*. Washington, DC: Georgetown University Press.

Alavi, Hamed; Khamichonak, Tatsiana (2017). EU and US Export Control Regimes for Dual Use Goods: an Overview of Existing Frameworks. In: Romanian Journal of European Affairs Vol.17 (1), pp. 59-74.

Amable, Bruno (2003). *The Diversity of Modern Capitalism*. Oxford: Oxford University Press.

Andreasson, Kim J. (ed.) (2012). *Cybersecurity. Public sector threats and responses*. Boca Raton Fla.: CRC Press (Public administration and public policy, 165).

Ansell, C.; Gash, A. (2007). *Collaborative Governance in Theory and Practice*. Journal of Public Administration Research and Theory, 8, p.543-571.

Bendiek, Annegret (2013). *Umstrittene Partnerschaft Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit*, SWP-Studien 2013/S 26, Stiftung Wissenschaft und Politik (SWP). Available online at: https://www.swp-berlin.org/publikation/cyberpolitik-transatlantische-zusammenarbeit/ (access on 27/11/2017).

Bendiek, Annegret (2016). *Sorgfaltsverantwortung im Cyberraum*, SWP-Studien 2016/S 03, Stiftung Wissenschaft und Politik (SWP). Available online at: https://www.swp-berlin.org/publikation/sorgfaltsverantwortung-im-cyberraum/ (access on 26/11/2017)

Busch, Nathan E.; Givens, Austen D. (2012). *Public-Private Partnerships in Homeland Security: Opportunities and Challenges*. In: Homeland Security Affairs Vol.8, Article 18.

Carr, Madeline (2016). *Public-Private Partnerships in national cyber-security strategies*. In: International Affairs Vol.92 (1), p. 43–62.

Cornish, Paul (2015). *Governing Cyberspace through Constructive Ambiguity*. In: Survival: Global Politics and Strategy, Vol. 57(3), pp. 153–176.

Cybersecurity Ventures. *Cybersecurity Market Report* (Q2 2017). Available online at: https://cybersecurityventures.com/cybersecurity-market-report/ (access on 28/11/2017).

Digitaltrends (24/08/2017). *Microsoft wins court case against Russian hackers, can take over their servers*. Article posted by Brad Jones. Available online at: https://www.digitaltrends.com/computing/microsoft-fancy-bear-russian-hackers/ (access on 28/11/2017).

Edgar/Manz (2017). Research Methods for Cyber Security. William Andrew Publishing.

Eichensehr, Kirsten E. (2017). *Public-Private Cybersecurity*. Texas Law Review Vol.95. Online available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847173 (access on 27/11/2017).

ECS - European Cyber Security Industrial Proposal for a contractual Public-Private Partnership (ECS cPPP), June 2016. Available online at: https://ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf (access on 28/11/2017).

European Commission, Press release (28/09/2016). *Commission proposes to modernise and strengthen controls on export of dual-use items*. Available online: http://europa.eu/rapid/press-release_IP-16-3190_en.htm (access on 27/11/2017).

European Parliament, EPRS Briefing Paper (28/09/2016). Review of dual-use export controls, EPRS: Available online: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf (access on 27/11/2017).

Gash, Alison (2016): Collaborative governance. In: Christopher K. Ansell und Jacob Torfing (Hg.): Handbook on Theories of Governance. Cheltenham, UK, Northampton, MA, USA: Edward Elgar, p. 454–467.

Gualmini, E.; Schmidt, V.A. (2013). *State transformation in Italy and France. Technocratic versus political leadership on the road from non-liberalism to neo-liberalism*. In: Schmidt, V.A.; Thatcher, M..*Resilient liberalism in Europe*, Cambridge: Cambridge University Press.

Guiora, Amos N. (2017). *Cybersecurity. Geopolitics, Law, and Policy*. Boca Raton: CRC Press.

Hall PA, Soskice D. (2001).*Varieties of Capitalism: The Institutional Foundations of Comparative Advantage*. Oxford: Oxford University Press.

Hancké, Bob; Rhodes,Martin and Thatcher, Mark (2007). *Beyond Varieties of Capitalism: Conflict, Contradictions, and Complementarities in the European Economy*, Oxford: Oxford University Press.

Herr, Trey; Rosenzeig, Paul (2015).Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model. In: Journal of National Security Law & Policy Vol.8 (2), pp.301-319.

Hiller, Janine S. (2014). *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 Santa Clara High Tech. L.J. 163 (2015).
Available online: http://digitalcommons.law.scu.edu/chtlj/vol31/iss2/1 (access on 26/11/2017).

Kouwenhoven, Vincent (1993). *Public Private Partnerships: A Model for the Management of Public Private Cooperation*. In: Kooiman, Jan (ed.), New Government-Society Interaction, London 1993.

Linder, Stephen H. (1999). *Coming to Terms With the Public-Private Partnership*. In: American Behavioral Scientist 43 (1), p. 35–51. DOI: 10.1177/00027649921955146.

Lyon, David (2006). *Theorizing surveillance. The panopticon and beyond*. Cullompton Devon: Willan Publishing.

Memorandum of Cooperation in the Field of Cybersecurity Japan & Israel (03/05/2017) Available online at: http://www.meti.go.jp/press/2017/05/20170508004/20170508004-5.pdf (access on 28/11/2017).

Microsoft Corporation. *Digital Crime Unit Factsheet*. Available online at: https://news.microsoft.com/download/presskits/DCU/docs/dcuFS_160115.pdf (access on 28/11/2017).

Microsoft Corporation (2015). *A Framework for cybersecurity information sharing and risk reduction*. Whitepaper available online: https://www.microsoft.com/en-us/cybersecurity/content-hub/information-sharing-framework-for-cybersecurity (access on 26/11/2017).

National Cyber Security Strategy Germany (2011), engl. Version. Available online at: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile (access on 28/11/2017).

National Cyber Security Strategy Finland (2013): Finland's Cyber Security Strategy. Government Resolutio – 24/01/2013. Secretary of the Security and Defence Committee, Finland (eg.), Helsinki, Finland.

National Cyber Security Strategy India (2013). National Cyber Security Policy. Available online at: http://164.100.94.102/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf (access on 28/11/2017).

National Cyber Security Strategy 2016 to 2021 - United Kingdom. Available online at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (access on 28/11/2017).

Nölke, Andreas; Brink, Tobias ten; Claar, Simone; May, Christian (2015): Domestic structures, foreign economic policies and global economic order. Implications from the rise of large emerging economies. In: European Journal of International Relations 21 (3), p. 538–567.

OECD (2012). *The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy*, OECD Digital Economy Papers, No. 209, OECD Publishing, Paris.

O'Leary, Rosemary; Vij, Nidhi (2012). *Collaborative Public Management: Where Have We Been and Where Are We Going?*, The American Review of Public Administration, Vol 42 (5), pp. 507 – 522

Privacy International (UK) (2016): Report: The Global Surveillance Industry. London, United Kingdom (Report). Available online at: https://www.privacyinternational.org/node/911 (access on 23/04/2017).

PwC Report (2016). Unlocking the cybersecurity growth potential Singapore's cybersecurity industry outlook. PricewaterhouseCoopers. Available online at: https://www.pwc.com/sg/en/publications/assets/unlocking-cybersecurity-growth-potential.pdf (access on 28/11/2017).

RUSI Report (2016). Public–Private Security Cooperation: From Cyber to Financial Crime. Royal United Services Institute for Defence and Security Studies, United Kindom. Available online at: https://rusi.org/publication/occasional-papers/public%E2%80%93private-security-cooperation-cyber-financial-crime (access on 28/11/2017).

Schmitt, Michael N.; Vihul, Liis (ed.) (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations. NATO Cooperative Cyber Defence Centre of Excellence*. First published 2017. New York, NY: Cambridge University Press.

SIPRI Yearbook 2017. *Armaments, Disarmament and international Security*, Stockholm International Peace Research Institute, Oxford University Press. Summary (multiple languages) available online: https://sipri.org/yearbook/2017 (access on 26/11/2017)

Thakuriah, Piyushimita; Tilahun, Nebiyou; Zellner, Moira (2017). *Seeing Cities Through Big Data. Research, Methods and Applications in Urban Informatics* (Springer Geography).

The Privacy Surgeon Report (2014): A Crisis of Accountability. A global analysis of the impact of the Snowden revelations. Online available at: https://cippic.ca/uploads/Snowden_at_one_year-global_survey.pdf (access on 20/04/2017).

Verma, Manisha (2016). *Role of State in Partnerships with the Private Sector*. In: Journal of Development Policy and Practice I (1), p. 53–70.

Wessels, Bridgette (2007). *Inside the digital revolution. Policing and changing communication with the public*, Routledge.

Wright, David; Kreissl, Reinhard (ed.) (2015). Surveillance in Europe. Routledge.

Wright, Steve (1998). STOA Report for the European Parliament. An Appraisal of Technologies of Political Control, Luxembourg. Available online at: http://www.statewatch.org/news/2005/may/steve-wright-stoa-rep.pdf (access on 28/11/2017).